

# TRADING BLOCKCHAIN Y CRIPTOECONOMÍA

La punta del iceberg



ALBERTO CARMONA | SERGIO PULIDO | DAVID ORELLANA

## **Tabla de contenido**

- **1. Introducción**
- **2. ¿Bitcoin o blockchain?**
  - 2.1. ¿Qué es Bitcoin?
  - 2.2. ¿Cómo lo hace?
  - 2.3. Historia del Bitcoin
    - 2.3.1. Inicios
    - 2.3.2. Primeros pasos
    - 2.3.3. Nacimiento de Mt. Gox y primeros problemas
    - 2.3.4. Silk Road
    - 2.3.5. Evolución hasta el momento actual
    - 2.3.6. La bifurcación de la comunidad
  - 2.4. Mecanismo de suministro de bitcoins
  - 2.5. Bitcoin: Burbuja o realidad
  - 2.6. La escalabilidad de Bitcoin
  - Conclusión
- **3. Blockchain**
  - 3.1. Transacciones
  - 3.2. Bloques
  - 3.3. Algoritmos de consenso
    - 3.3.1. Prueba de trabajo o Proof of work (PoW):

- 3.3.2. Prueba de participación (Proof of Stake o PoS)
- 3.3.3. Mecanismo híbrido PoW/PoS
- 3.3.4. Prueba de participación delegada (Delegated Proof of Stake o dPoS)
- 3.3.5. Tolerancia delegada ante fallo bizantino (delegated Byzantine Fault tolerance o dBFT)
- 3.4. El trilema de las blockchain
- 3.5. Redes blockchain públicas y privadas
  - 3.5.1. ¿Qué características tiene una blockchain privada?
- 3.6. Hyperledger
  - 3.6.1. Proyectos de Hyperledger
    - 3.6.1.1. Frameworks de Hyperledger
    - 3.6.1.2. Módulos de Hyperledger
- 3.7. Casos de uso del Blockchain
- Conclusión
- **4. Ethereum y más**
  - 4.1. Ethereum
  - 4.2. Clasificación de los activos digitales
    - 4.2.1. Criptomonedas o criptodivisas
    - 4.2.2. Plataformas
    - 4.2.3. Tokens
  - 4.3. Inflación y deflación

Más libros de trading en :  
<https://t.me/tradingpdfgratis>

- 4.3.1. Inflación en las criptomonedas
- 4.4. Criptomonedas más importantes
- 4.5. Qué es una ICO
- 4.6. Cómo analizar una ICO
- 4.7. Qué es una STO
- 4.8. Carteras
- Conclusión
- **5. Trading básico**
  - 5.1. Tipos de Análisis
    - 5.1.1. Análisis fundamental
    - 5.1.2. Análisis técnico
  - 5.2. Trading avanzado
    - 5.2.1. Scalping
    - 5.2.2. Arbitraje
    - 5.2.3. Futuros
    - 5.2.4. Trading algorítmico
    - 5.2.5. Backtesting
    - 5.2.6. Websockets y API REST
  - 5.3. Gestión del riesgo
    - 5.3.1. Apalancamiento
    - 5.3.2. Stop Loss

- 5.4. ¿Por qué es importante diversificar?
- 5.5. Rebalancear la cartera
- Conclusión
- **GLOSARIO**

Más libros de trading en :  
<https://t.me/tradingpdfgratis>

© Alberto Carmona Sánchez, David-Conelly Orellana Huhn y Sergio Pulido Grima, 2019



Impresión:



[unoeditorial.com](http://unoeditorial.com)

La reproducción total o parcial de este libro, por cualquier medio,  
no autorizada por los autores y editores viola derechos reservados.

Cualquier utilización debe ser previamente autorizada.

Más libros de trading en : <https://t.me/tradingpdfgratis>

# 1. Introducción

En el último año, prácticamente todos los días hemos visto en las noticias que se hablaba de *blockchain*. Una y otra y otra vez más. Y, como suele ser habitual, intentamos entender un poco en qué consiste la tecnología, y no es fácil. No solo eso, sino que, además, leemos cosas que parecen opuestas entre sí.

Estas contradicciones entre fuentes suceden por lo siguiente. Estamos hablando de una revolución tecnológica considerable. Por primera vez existe una forma fiable de realizar transacciones entre personas sin necesidad de una entidad intermediaria que se haga responsable del proceso. No es fácil aprender sobre *blockchain*, hay que dedicarle mucho tiempo y tener un cierto *background* tecnológico ayuda. Pero, aun así, se requieren meses de esfuerzo para ver más allá de la punta del iceberg. De ahí que veamos tantas contradicciones en los medios de comunicación. Por un lado, la falta de tiempo para formarse en el tema. Y, por otro, lo difícil que es explicar en qué consiste, en poco espacio, y sin usar jerga continuamente. Todo un reto.

Las criptomonedas, que existen gracias a la tecnología *blockchain*, han experimentado unas revaloraciones increíbles. Esto las ha colocado en el punto de mira de los medios de comunicación, y tanto las empresas como los individuos hemos tratado de buscar ideas donde aplicar esta tecnología y generar un nuevo modelo de negocio disruptivo.

Miles de personas se han adentrado en este mundo a través del *trading*. Los

volúmenes de mercado en crecimiento y una fuerte volatilidad han sido los catalizadores perfectos para que estos operadores se abalanzaran en masa y consiguieran rentabilidades astronómicas. Esto, a su vez, ha reforzado que el sector tuviera más presencia en los medios de comunicación, generándose una retroalimentación. Cuanto más se hablaba del tema, más gente entraba al mercado, y cuanta más gente entraba al mercado, más crecían las cotizaciones.

Este *hype* que hemos visto es habitual que se dé con los avances tecnológicos más punteros. Así fue con Big Data, con la Realidad Virtual, con la Inteligencia Artificial, y un largo etcétera. Tendemos a sobrevalorar los efectos de una tecnología en el corto plazo y a infravalorarlos en el largo plazo. De ahí que pasemos por una fase de optimismo irracional para después acabar en el llamado abismo de la desilusión.

Con blockchain estamos viviendo este ciclo. Puede que lo hayamos experimentado de forma más abrupta, ya que, en este caso, se ha puesto la atención en la tecnología cuando se han disparado las cotizaciones de las criptomonedas. Pero ahora, un año más tarde de los máximos históricos de diciembre de 2017, nos estamos enfrentando a una dura realidad. Blockchain no es la solución a todos nuestros problemas. Bienvenidos al mencionado abismo de la desilusión.

Pero esto es una buena noticia, aunque no lo parezca. Porque, en este tiempo, la investigación y el desarrollo se ha multiplicado, y prácticamente cualquier empresa de cierto tamaño se ha visto obligada a dedicar a un departamento a estudiar qué implicaciones puede tener sobre el negocio.

El conocimiento colectivo que tenemos sobre esta tecnología se ha disparado. Y

es así como se conseguirá seguir desarrollándola para que realmente se convierta en algo útil y esté instaurada en nuestras vidas en unos pocos años. Esta tecnología nace como *open source*, es decir, miles de personas en el mundo están viendo exactamente el mismo código y pueden detectar errores, buscar mejores soluciones y aportar para que el desarrollo siga evolucionando. Esto choca con la forma tradicional de crear productos o servicios, donde cada empresa lucha por mantener una propiedad intelectual que les permita explotar económicamente el desarrollo. Cualquier persona del mundo puede aportar al código de cientos de proyectos basados en esta tecnología. El potencial de esta forma de trabajar es increíble. Los pasos que se dan son gigantescos gracias a la colaboración desinteresada de expertos de cualquier lugar del mundo.

Volviendo al estado actual, durante el 2018 pudimos conocer decenas de empresas dedicándose a realizar pruebas de concepto para decidir si instaurar blockchain en alguna parte de sus procesos. Y las grandes firmas informáticas están ofreciendo ya soluciones *Blockchain as a Service*. Se puede implantar esta tecnología de forma relativamente sencilla, teniendo en cuenta el estado del arte actual.

Pronto, muy pronto, veremos un aluvión de noticias de cómo ya ciertas empresas están utilizándola en su cadena de suministro, en su contabilidad interna, en su gestión de inventarios... Porque una vez que haya un pionero que la aplique, el resto de competidores no querrá quedarse detrás.

Y la razón por la que hemos decidido escribir este libro es la siguiente. Estamos ante una revolución que aún no sabemos hasta dónde puede llegar. Y cada vez más amigos y familiares nos vienen a preguntar sobre blockchain y las implicaciones que puede tener. Nos encanta ver cómo se despierta su interés. Así

que dijimos: ¿por qué no les ponemos más facilidades y les escribimos un libro con el cual puedan empezar a entender un poco mejor todo este ecosistema?

Más libros de trading en : <https://t.me/tradingpdfgratis>

## 2. ¿Bitcoin o blockchain?

Los términos Bitcoin y blockchain siempre van de la mano, y cuando uno aterriza en este sector al principio no entiende dónde están las diferencias, y es totalmente normal. La razón es que Bitcoin es el primer caso de aplicación de la tecnología blockchain de forma exitosa.

A día de hoy existen más de 2.000 criptomonedas<sup>[1]</sup>, pero la más antigua y conocida es Bitcoin. Además, su capitalización de mercado (el precio de cada moneda multiplicado por la cantidad de monedas en circulación) se encuentra alrededor del 50% del mercado total de criptomonedas, es decir, este protocolo es tan grande como las otras 2.000 criptomonedas existentes.

### 2.1. ¿Qué es Bitcoin?

Bitcoin es la primera aplicación de tecnología blockchain que soluciona un problema existente desde hace muchos años. Permite realizar transacciones de dinero digital entre personas sin que tengan que confiar entre sí ni en ninguna entidad intermediaria.

Bitcoin es un protocolo propuesto en 2008 por una persona (o grupo de personas) bajo el pseudónimo de Satoshi Nakamoto. No pensemos que sucedió de una forma muy elegante, ni que fue un lanzamiento mundial anunciado a bombo y platillo. Simplemente esta persona publicó un *whitepaper* (un

documento técnico que aborda un problema y una posible solución) en una lista de distribución de correo acerca de criptografía<sup>[2]</sup>.

Este whitepaper se titulaba *Bitcoin: Un sistema de dinero en efectivo electrónico peer-to-peer*. A continuación, seguía con el siguiente texto:

*Una versión puramente peer-to-peer de dinero electrónico permitiría que los pagos online fueran enviados directamente por una parte a la otra sin pasar a través de una institución financiera. Las firmas digitales proveen parte de la solución, pero el principal beneficio se pierde si se requiere que un tercero confiable para evitar el doble gasto. Proponemos una solución al problema del doble gasto utilizando una red peer-to-peer. La red sella mediante timestamps las transacciones en una cadena continua de prueba de trabajo basada en hash, formando un registro que no puede ser modificado sin rehacer la prueba de trabajo. La cadena más larga no solo sirve como prueba de la secuencia de los eventos sucedidos, sino que además demuestra que proviene de la mayor agregación de poder de cálculo CPU. Mientras la mayoría de la capacidad de cálculo CPU esté controlada por nodos que no estén cooperando para atacar la red, generarán la cadena más larga superando a los atacantes. La red en sí requiere una infraestructura mínima. Los mensajes se propagan en base a «mejor esfuerzo» y los nodos pueden abandonar y volver a unirse a la red a voluntad, aceptando la cadena de prueba de trabajo más larga como prueba de lo que ha sucedido en su ausencia.*

Si no hemos entendido nada del texto anterior, no nos preocupemos todavía.

Vamos a explicar a lo largo del libro qué es el doble gasto, la prueba de trabajo, los *timestamps*, y mucha más terminología clave para entender Bitcoin y blockchain.

Satoshi publicó el whitepaper después de haber programado el sistema. Él mismo decía que tenía que verlo en funcionamiento antes de convencerse de que podía resolver los problemas planteados. Difícilmente se podría imaginar lo que iba a pasar en estos años y la revolución que Bitcoin ha supuesto, y no solo en el ámbito financiero.

Como curiosidad, Satoshi Nakamoto en este whitepaper nunca menciona la palabra blockchain, sino que hace referencia a «bloques que pasan a formar parte de una cadena». El término blockchain se popularizó años más tarde.

## **2.2. ¿Cómo lo hace?**

La tecnología que hay detrás de Bitcoin es blockchain. Básicamente, blockchain es un registro de transacciones público y distribuido. Mantiene la información acerca de todas las operaciones que han sucedido y es constantemente actualizado añadiendo las nuevas transacciones que van ocurriendo.

Cualquier persona puede descargarse en su ordenador el cliente de Bitcoin y ejecutarlo. De esta forma pasaría a ser un nodo, es decir, un ordenador que aloja una copia completa de la blockchain y añade nuevos bloques a la cadena de forma coordinada con el resto de nodos de la red.

Es distribuido porque cualquier persona puede descargarse este registro y

mantendrá la misma copia que los demás. Todas las copias se actualizan a la vez con los movimientos que vayan sucediendo.

Y es pública porque cualquier usuario puede participar en la red y realizar transacciones. No hay nadie que pueda restringir el acceso de otra persona a esta tecnología, ni hay que registrarse en ningún lugar, ni dar datos personales. Simplemente con descargarnos un software podemos crear una cartera propia donde se guardarán nuestros bitcoins. Y podremos enviar y recibir bitcoins libremente, sin que nuestra operación sea censurada.

La tecnología blockchain actúa además como un registro inmutable. Las operaciones que suceden en la red son agrupadas en bloques, y estos son validados y unidos al bloque anterior, formando una cadena. Una vez que un bloque se añade a la cadena, no puede ser eliminado ni alterado. Podemos ver todas las transacciones que han tenido lugar desde el origen hasta este momento, y sabemos que lo que estamos viendo es un registro que no puede ser manipulado.

Lo verdaderamente revolucionario es que, gracias a la criptografía (técnicas de cifrado para realizar comunicaciones seguras), se pueden ejecutar estas transacciones y matemáticamente comprobar su veracidad sin necesidad de intermediarios ni de una autoridad que las valide.

Entendamos bien este punto, pues es la verdadera revolución.

Hasta ahora, cualquier transacción económica dependía de autoridades financieras. Cuando queremos realizar un intercambio con otra persona, tendremos que usar nuestra cuenta del banco, y este se encarga de anotar los cambios en sus libros de cuentas. Es decir, si enviamos dinero, nos lo resta en

nuestra cuenta y lo suma en la de destino. Apuntes contables y nada más.

Esto nos cuesta tiempo y dinero. ¿Cuántos días tarda una transferencia internacional, y cuánto nos cobran por ella? Con los avances tecnológicos de los que disfrutamos a día de hoy, esto es una ineficiencia muy significativa.

Imaginemos, además, que estamos en un país en el que el gobierno decide de forma arbitraria perseguir a un colectivo concreto. Nuestras cuentas (que nunca estuvieron en nuestra propiedad, no lo olvidemos) estarán bloqueadas. Nuestros ahorros, inaccesibles.

¿Cómo hemos llegado a perder el control sobre algo tan importante como nuestro propio dinero?

La función que cumplen a día de hoy los bancos es la de ser intermediarios de confianza. Sabemos que podemos enviar dinero, que no va a desaparecer. Sabemos que, a final de mes, la nómina aparecerá reflejada en nuestra cuenta. Sabemos que eso pasará siempre, sin importar la política, la economía, o cualquier evento mundial. O más bien **queremos pensar** que esto es así. Pero la realidad nos muestra una y otra vez que estos organismos no son confiables, y pueden actuar motivados por intereses propios. Y que los gobiernos imponen restricciones arbitrarias a los movimientos de capitales si lo desean.

Bitcoin resuelve el problema de transferir valor económico sin necesidad de terceros de confianza. Depositamos nuestra confianza en un algoritmo matemático que verifica las operaciones. Nuestras cuentas serán nuestras siempre. Nadie puede impedirnos que abramos una cuenta, ni bloquearnos el acceso a ella, ni que enviemos o recibamos dinero.

Además, sabemos que existe un suministro limitado de monedas y que nadie

puede decidir elevarlo ni disminuirlo. En las economías actuales no sabemos al ritmo que los bancos centrales imprimen dinero, ni el suministro total existente. Cada dólar o euro que sale de la máquina hace que nuestros ahorros valgan un poquito menos. Esta erosión continua hace que nos empobrezcamos a largo plazo.

Por tanto, cuando decidimos participar en una economía como Bitcoin sabemos que el suministro no es manipulable, y que da igual que haya actores deshonestos en la red, porque la confianza la depositamos en unos algoritmos y no en unas entidades.

Antes de continuar, vamos a puntualizar un aspecto necesario para la nomenclatura. Esto es válido tanto para Bitcoin como para el resto de protocolos:

◇ Bitcoin, con mayúscula, es el software, la tecnología.

◇ bitcoin, con minúscula, es la unidad monetaria, lo que enviamos y recibimos.

Por tanto, si estamos hablando de la tecnología, de la plataforma o de la red utilizaremos la primera. Cuando hablemos de lo que podemos intercambiar, será la segunda.

El funcionamiento básico de Bitcoin es muy sencillo:

Alicia quiere enviarle a Bruno un bitcoin. Para ello hace lo siguiente:

- ▶ Alicia mira en su cartera si tiene fondos disponibles. Una cartera es una dirección dentro de la blockchain. Solo puede ordenar transferencias la persona que tenga la clave privada de esa dirección.
- ▶ Como tiene fondos en su cartera, ordena la transferencia de un bitcoin a la

cartera de Bruno.

- Esta operación se agrupa junto a cientos de operaciones más y forman un bloque.

Ahora viene una parte más compleja:

- Para que el bloque pase a formar parte de la cadena de bloques, y la operación de Alicia se ejecute, dicho bloque tiene que ser verificado criptográficamente. Este proceso se llama minado (lo describiremos más adelante) y nos asegura que todas las operaciones son legítimas y se ajustan al protocolo.
- Una vez que el bloque ha sido minado, pasa a formar parte de la blockchain. Desde el momento en que Alicia ordena la transferencia, no puede revertir la operación. Cuando el bloque ya forma parte de la blockchain, Bruno puede comprobar que en su cartera ha aparecido un bitcoin, y podrá a su vez enviarlo si lo desea. A partir de ahora, este bitcoin pertenece únicamente a Bruno, y solo él podrá utilizarlo mediante sus claves, ninguna otra persona podrá retirarlo de su cuenta.

Gracias a este proceso criptográfico, Alicia y Bruno pueden realizar transacciones sin tener que recurrir a una autoridad de confianza como un banco. Es tan sencillo como que ambos tienen la certeza de que Alicia ha enviado el bitcoin a Bruno, y no puede deshacer la operación ni enviar ese mismo bitcoin a otra dirección a la vez.

## **2.3. Historia del Bitcoin**

Como toda buena historia, los inicios de Bitcoin están envueltos en misterio. Hay bastantes hechos de los que tenemos certeza, como la creación del primer bloque de la cadena, o la primera transacción. Es lo bonito de las blockchain, lo que sucede en ellas permanece de forma inmutable en el tiempo. Pero respecto al autor o autores hay poca información, más allá de los correos que escribían, contribuciones en foros y, por supuesto, de su obra maestra que aún sigue viva.

Por ponernos un poco en contexto. La comunidad cypherpunk lleva trabajando desde hace muchos años en mejorar la privacidad del individuo frente a gobiernos y corporaciones. La forma de hacerlo es mediante mensajería encriptada, e idealmente un sistema de transacciones económicas de carácter anónimo.

En su *Cypherpunk's Manifesto*<sup>[3]</sup>, Eric Hughes dice lo siguiente:

*La privacidad es necesaria en una sociedad abierta en la era electrónica. Privacidad no es secretismo. Un asunto privado es aquello que no queremos que sepa todo el mundo, un asunto secreto es aquello que no queremos que sepa nadie. La privacidad es el poder de revelarse uno mismo selectivamente al mundo.*

*[...]*

*No podemos esperar que gobiernos, corporaciones y otras grandes entidades sin rostro nos garanticen la privacidad sin obtener nada a cambio. Les resulta beneficioso hablar de nosotros, y debemos esperar que lo hagan. Intentar impedir que hablen es luchar contra las realidades de la información.*

La privacidad es el derecho de que nuestros datos no sean utilizados sin nuestro

consentimiento. Y la realidad es que cada vez tenemos menos privacidad, en nombre de la libertad (irónicamente). Para estar más seguros, tenemos que dar más y más información a los gobiernos.

¿Y cómo nos protegemos cuando son estos los actores maliciosos?

Hay muchos ejemplos a día de hoy de represión debido a orientación sexual, ideología, religión, etc. Cuanta más información estemos obligados a compartir con las autoridades, más vulnerables somos.

Cuando a esta comunidad cypherpunk se les presenta una moneda cuasi-anónima, fuera del control de gobiernos y regida exclusivamente por la oferta y la demanda, cuyo funcionamiento es incensurable, el proyecto tiene una acogida muy calurosa por la expresión de libertad que supone.

### **2.3.1. Inicios**

Se rumorea que Satoshi Nakamoto empezó a desarrollar esta tecnología en Japón, alrededor de 2007. Como se trata de un pseudónimo, no podemos saber si es una persona o varias, ni dónde se encontraba realmente. Y da lo mismo, su deseo era permanecer anónimo.

En cualquier caso, el 18 de agosto de 2008 se registra el dominio Bitcoin.org. El día 1 de noviembre de ese mismo año, envió un correo electrónico a una lista de distribución de criptografía<sup>[4]</sup> el siguiente mensaje:

*He estado trabajando en un nuevo sistema de dinero electrónico entre pares (peer-to-peer o p2p), sin terceros de confianza.*

*El documento se encuentra disponible en:*

*<http://www.bitcoin.org/bitcoin.pdf>*

*Las propiedades principales:*

- ▶ *El doble gasto se previene mediante una red peer-to-peer.*
- ▶ *Sin necesidad de partes confiables.*
- ▶ *Los participantes pueden ser anónimos.*
- ▶ *Las nuevas monedas se generan por una prueba de trabajo similar a Hashcash.*
- ▶ *La prueba de trabajo para la generación de nuevas monedas también potencia la red para prevenir el doble gasto.*

A partir de este correo se genera un debate en el que Satoshi va contestando dudas que le plantean. En este grupo se encontraba Hal Finney, que ya había diseñado un sistema de prueba de trabajo similar al utilizado por Bitcoin. Además, Hal fue la primera persona en recibir una transacción de esta red y estuvo muy involucrado en el desarrollo durante los primeros años.

Tras varios meses de debate, el 3 de enero se crea el bloque génesis<sup>[5]</sup> de Bitcoin. Este bloque marca el comienzo de una blockchain y, en este caso, el creador incluyó el siguiente mensaje:

**«The Times 03/Jan/2009 Chancellor on brink of second bailout for banks».**

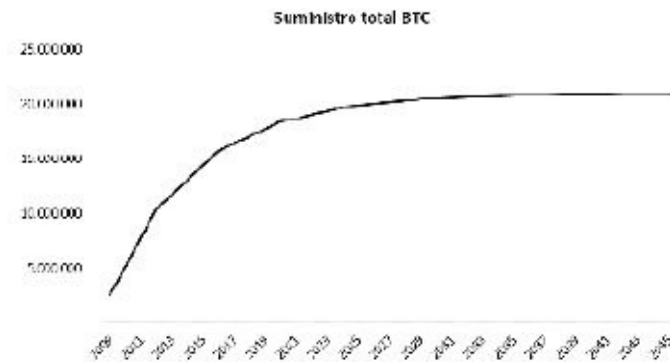
Es el titular del periódico *The Times* de aquel día. Resulta una ironía que el titular del día que nace Bitcoin trate acerca de un rescate bancario. Pone de relieve que el actual es un sistema fallido, y Bitcoin surge como alternativa al

control de los bancos centrales y gobiernos. No olvidemos que esta tecnología tiene orígenes libertarios, y que es una forma de luchar contra el sistema establecido.

Este mensaje seguramente cumpla también con una segunda función, sirve como marca de tiempo. Es una forma de asegurar que ese bloque génesis nació ese día y no antes.

El siguiente bloque<sup>[6]</sup> fue minado el día 9 de enero. En promedio, un bloque debería de minarse cada 10 minutos. Es posible que este retraso ocurriera por la siguiente razón. El titular del que acabamos de hablar era perfecto para dar nacimiento a la red, pero aún le quedaban algunos ajustes que hacer al protocolo. Es posible que aprovechara la situación para comenzar la cadena, pero no dejó la máquina minando de tal forma que pudiera seguir implementando las últimas modificaciones en el programa.

Sea por la razón que fuera, ese día volvió a enviar un correo a la lista de distribución anunciando el lanzamiento del software, en la versión 0.1.0, disponible para ser descargado por cualquiera. Y además aprovechó este correo para explicar el suministro total de bitcoins. Este sería de 21 millones, generándose 10,5 millones de bitcoins entre los cuatro primeros años, la mitad los cuatro siguientes, y así hasta llegar al máximo situado en esos 21 millones. Este sistema lo que hace es reducir la recompensa a los mineros a la mitad cada 210.000 bloques. De 50 BTC por bloque a 25, a 12,5, a 6,25... y así. Se conoce al proceso como *halving*, que viene del término inglés *half* (mitad).



*Fuente: Elaboración propia*

En 2018 se terminó el año con aproximadamente un 83% minado sobre el suministro total (cerca de los 17,5 millones de bitcoins). En el año 2045 se habrían minado el 99,9%, emitiéndose en ese periodo de cuatro años 20.500 más. A partir de 2110 se podría considerar que ya se han minado los 21 millones, ya que habría en circulación unos 20.999.999,53 bitcoins.

Tras el correo de Satoshi, el primero en responder es nuevamente Hal Finney, siendo posiblemente la primera persona en descargarse el software y empezar a utilizarlo.

El día 12 de enero, en el bloque número 170, se produce la primera transacción de la red entre Satoshi y Hal.

¿Os imagináis tener un registro fiable de todas las transacciones en cada una de las monedas tradicionales que conocemos? Gracias a la blockchain podemos ver todas las operaciones que han tenido lugar desde su creación hasta el momento actual.

Más libros de trading en : <https://t.me/tradingpdfgratis>

### 2.3.2. *Primeros pasos*

Poco a poco, Satoshi da a conocer su obra en distintos foros y comienza el interés en su software. Empiezan los debates relativos a la seguridad de la red, a cómo se conseguirá una adopción masiva y a la forma de calcular el valor real que tiene el Bitcoin.

El 5 de octubre de 2009, un usuario conocido como NewLibertyStandard<sup>[7]</sup> establece el siguiente precio: **1\$ = 1.309,03 BTC**

El cálculo anterior se realizó teniendo en consideración el consumo eléctrico que tenía un ordenador minando un bitcoin.

El 16 de diciembre, casi un año más tarde de la publicación del primer cliente de Bitcoin, Satoshi anuncia la primera actualización, en su versión 0.2. Poco después, el 30 de este mes, se produce el primer incremento en la dificultad de la red. La dificultad es variable en función de la capacidad de minado total de la red, de tal forma que el promedio para resolver un bloque sea siempre de 10 minutos. Esto significa que cada vez más gente estaba poniendo su ordenador a minar en la red, y que crecía el interés en la tecnología.

El 15 de enero de 2010, un usuario de Bitcointalk llamado dwdollar publica<sup>[8]</sup> su intención de crear el primer *exchange* donde se pudieran intercambiar bitcoins. Un exchange es el lugar donde podemos comprar y vender criptomonedas.

Durante un tiempo están en pruebas con cuentas ficticias, hasta que finalmente el 16 de marzo decide empezar el trading con dinero real. Es curioso que tan solo un año más tarde de nacer Bitcoin, ya había mucha gente que empezó a ver el potencial que tenía e incluso crearon una plataforma para comprarlos y

venderlos.

El 18 de mayo tenemos otro evento importante en la historia del Bitcoin. Un usuario de ese mismo foro, llamado Laszlo<sup>[9]</sup>, se ofrece a pagar 10.000 bitcoins a quien le envíe dos pizzas a su casa. Esta transacción tuvo lugar el 22 de mayo, y actualmente todos los años se celebra este día y es conocido como Bitcoin Pizza Day.

Y un poco más tarde llega la primera explosión en el precio del bitcoin. El 7 de julio se publica la versión 0.3. y el día 10, un usuario la sube al foro slashdot<sup>[10]</sup>. A raíz de este evento, BTC experimenta durante los siguientes días un incremento en su valor de diez veces, pasando de 0,008 a 0,08 USD/BTC.

### ***2.3.3. Nacimiento de Mt. Gox y primeros problemas***

Jed McCaleb es otra de las personas de peso en el mundo blockchain. En su momento creó la aplicación eDonkey2000 (para descargar contenidos digitales p2p). El 17 de julio de 2010 decidió abrir una plataforma para comprar bitcoins con dólares llamada Mt. Gox.

Como curiosidad, este dominio lo había utilizado anteriormente para intentar crear un mercado digital para que los jugadores de Magic: The Gathering Online pudieran comprar y vender sus cartas como si fuera un mercado de acciones. De hecho, el nombre del dominio corresponde a «**Magic: The Gathering Online Exchange**».

Este exchange sería el más conocido durante muchos años, ya que acaparó el

70% del volumen de transacciones, y fue más conocido aún por las vulnerabilidades que sufría. Volveremos a hablar de él en varias ocasiones. De momento, quedémonos con que fue fundado en esta fecha.

Por primera vez, la red Bitcoin se iba a encontrar con un problema muy grave. El 15 de agosto de 2010, en el bloque 74.368, un *exploit* (una vulnerabilidad del software que se puede explotar maliciosamente) permite generar 184 mil millones de bitcoins. Un usuario se da cuenta y lo publica en Bitcointalk<sup>[11]</sup>. La única solución posible era hacer un *fork*, es decir, volver a un punto anterior de la cadena donde esa transacción aún no se había realizado, solucionar el fallo que permitió dicho exploit, y continuar como si nada hubiera pasado. De esta forma, como los mineros dejan de trabajar en la cadena «errónea», las monedas creadas no serían aceptadas por nadie y no podrían gastarse.

Tan solo cinco horas más tarde, Satoshi publicó<sup>[12]</sup> la versión que solucionaba este problema. Gracias al apoyo de la comunidad, se consiguió dejar esta transacción errónea en una cadena huérfana y evitar el daño que podría haber causado. Para que esta solución fuera efectiva, los mineros tenían que adoptar el nuevo software, y empezar a calcular la blockchain en un punto previo al bloque donde se provocó el exploit, para volver a empezar a generar bloques desde ese momento.

Otra vulnerabilidad fue descubierta y parcheada rápidamente el 29 de septiembre. Fue expuesta por el usuario kermi en el mismo foro<sup>[13]</sup>, lugar donde, por aquel entonces, se encontraban las personas más implicadas con el desarrollo de Bitcoin.

Siendo este software cada vez más conocido por la gente, se empiezan a realizar

decenas de eventos y con ellos el precio del bitcoin vuelve a coger un gran impulso pasando de los 0,064 USD/BTC el 7 de octubre de 2010, a los 0,5 USD/BTC el 31 de enero de 2011.

¡Para finales de año Bitcoin ya superaba la capitalización de 1 millón de dólares<sup>[14]</sup>!

#### **2.3.4. Silk Road**

Hasta este momento Bitcoin era una red utilizada por desarrolladores, libertarios, criptógrafos y cypherpunks. Pero esto estaba a punto de cambiar. En febrero de 2011 nace Silk Road, el portal de internet conocido como el eBay de la droga.

Fue creado por el americano Ross Ulbricht, que se definía de la siguiente forma en su perfil de LinkedIn<sup>[15]</sup>:

*Me encanta aprender y usar constructos teóricos para entender mejor el mundo que me rodea. Por ello estudié Física en la universidad y trabajé como investigador durante cinco años. Publiqué mis descubrimientos en revistas especializadas cinco veces durante ese periodo, primero sobre células solares orgánicas y después sobre cristales de lámina delgada. Mi meta durante este periodo de la vida fue simplemente expandir la frontera del conocimiento humano.*

*Ahora mis objetivos han cambiado. Quiero usar la teoría económica como un medio para abolir el uso de coacción y de la agresión contra el ser humano. Igual que la esclavitud ha sido abolida en casi todos los*

*lugares, creo que la violencia, coacción, y todo uso de fuerza de una persona sobre la otra puede terminarse. El más expandido y sistémico uso de fuerza sucede entre las instituciones y gobiernos, así que este es mi punto de esfuerzo actual. La mejor forma de cambiar un gobierno es cambiando la mente de los gobernados. Con ese fin, estoy creando una simulación económica para darle a la gente una experiencia de primera mano de cómo sería vivir en un mundo sin el uso sistémico de la fuerza.*

Así es como nace el portal Silk Road. Se trataba de un mercado libre en la *Deep web*, donde se podía comprar todo tipo de droga. Las transacciones se realizaban en bitcoins, ya que permitían el anonimato necesario. En la plataforma estaba prohibida la venta de pornografía infantil, de tarjetas de crédito robadas, compraventa de armas y la contratación de asesinos.

Este mercado llegó a mover más de mil millones de dólares.

Desde prácticamente el momento en el que fue creado, el FBI empezó a investigarlo con el objetivo de dar con el creador y los vendedores. Pero gracias a la red Tor, tardaron años en conseguir reunir suficiente información sobre Ulbricht. Lo lograron gracias al rastro de sus alias en distintos foros, hasta que dieron con uno de ellos con el que publicó su correo personal. Este fallo permitió al FBI capturarlo en San Francisco, mientras estaba logueado como administrador en Silk Road. Encontraron en su poder millones de dólares en bitcoins, y un diario privado que contenía suficiente evidencia para culparlo.

En cualquier caso, el juicio posterior fue bastante controvertido. Se violaron varios derechos fundamentales del acusado, se utilizaron pruebas falsas, y se ocultó al jurado que dos miembros del FBI corruptos habían estado involucrados

en el caso. Estos dos acabaron en prisión un año más tarde por lavado de dinero, extorsión, y obstrucción a la justicia.

La acusación más grave que recayó sobre Ulbricht fue la de seis intentos de asesinato mediante la contratación de sicarios. Aunque las pruebas nunca llegaron a ser presentadas en el juicio, el juez permitió al abogado de la acusación utilizar este argumento ante el jurado<sup>[16]</sup>. Debido a ello, la sentencia fue de dos cadenas perpetuas a pesar de solo ser acusado de crímenes no violentos. El 26 de julio de 2018 el gobierno finalmente desestimó los cargos por asesinato<sup>[17]</sup>.

Esta historia tiene mucha importancia, ya que puso en los grandes medios de comunicación por primera vez la palabra Bitcoin.

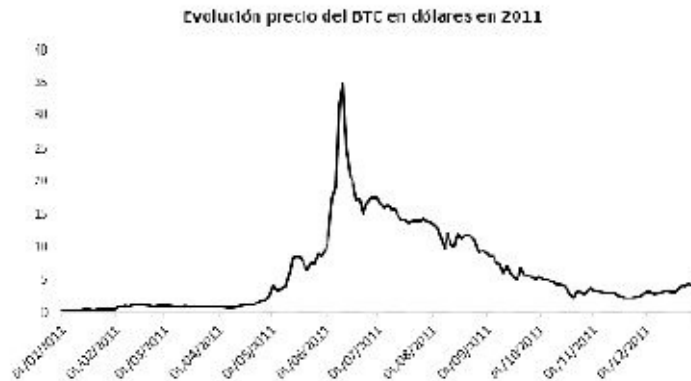
En paralelo con estos sucesos, el precio de la criptomoneda sigue subiendo hasta superar el dólar, se van creando cada vez más pools de minado<sup>[18]</sup>. Y Jed vende Mt. Gox a Mark Karpelès, miembro fundador de la Bitcoin Foundation, que tenía como objetivo promocionar y estandarizar Bitcoin.

### ***2.3.5. Evolución hasta el momento actual***

La evolución del bitcoin durante el 2011 fue frenética, pasó de 30 céntimos a un dólar, de un dólar a 10 dólares, y de 10 dólares a 35. Pocos días más tarde, comenzó su rápido descenso hasta los 15 dólares, para acabar el año bajando lentamente hasta los 5.

La caída de 32 a 15 dólares coincide con el mayor robo de bitcoins de una

cartera hasta ese momento, esta cartera contenía 25.000 bitcoins.



Fuente: <https://www.blockchain.com>

Mt. Gox, ya en manos de Mark Karpelès, sufre su primer hackeo. El 19 de junio de 2011 un intruso logra que el precio del bitcoin en la plataforma caiga desde los 17,5 dólares a un céntimo, resultando en un impacto de casi 9 millones de dólares a las cuentas comprometidas<sup>[19]</sup>.

Durante este año siguen sucediendo hackeos en distintos exchanges, la dificultad de la red sigue subiendo, y cada vez hay más *pools* de minería. La adopción de Bitcoin sucede de forma rápida y empiezan a desarrollarse muchos negocios basados en esta tecnología.

En junio de 2012 se funda Coinbase. Fue una de las primeras empresas que permitió comprar bitcoins con dólares, y actualmente es una de las más importantes del sector. En 2017 sus ingresos superaron el billón de dólares<sup>[20]</sup>, y se estima que la mitad de ese ingreso se logró en diciembre de ese año. Ya en el mes de noviembre se estimaba que crecían a un ritmo aproximado de 100.000

usuarios nuevos al día<sup>[21]</sup>.

Esta empresa es de las que más duramente está trabajando con el objetivo de acercar las criptomonedas al mundo tradicional. Una de las principales barreras a superar si queremos que el día de mañana haya una adopción masiva, es la de la usabilidad. El proceso de compra y custodia de criptoactivos tiene que ser sencillo y seguro. Es la única forma de que se llegue a un público general.

Durante este año, las noticias más recurrentes son de hackeos y más hackeos. La centralización de bitcoins en los exchanges hacen que se conviertan en un objetivo natural de los atacantes.

Y un año más tarde, en 2013, el bitcoin sigue con su ascenso meteórico, pasando de poco más de 10 dólares a superar los 1.100 en noviembre.



Fuente: <https://www.blockchain.com>

En diciembre de ese año sucedió el mayor robo de bitcoins hasta el momento. Tuvo lugar en Sheep Marketplace, un mercado similar al ya cerrado Silk Road. El ladrón logró hacerse con 96.000 bitcoins.

Y, finalmente, es en 2014 cuando Mt. Gox se ve obligada a cerrar. Pasaron un 2013 muy duro, debido a problemas regulatorios y técnicos. Varias veces suspendieron los retiros, siendo el plazo aproximado de unos tres meses para recuperar el dinero depositado en la plataforma.

El 7 de febrero de 2014 pausaron de forma indefinida los retiros. El 24 suspendieron la actividad de trading y la página web quedó inaccesible<sup>[22]</sup>. Y ese mismo día se filtró un borrador interno<sup>[23]</sup> con diferentes alternativas para gestionar la crisis por parte de la empresa. Con el paso de los años, 744.408 bitcoins habían sido robados.

Al día siguiente se declararon en bancarrota en Japón, donde estaban ubicadas las oficinas. El CEO Mark Karpelès fue arrestado en agosto de 2015, acusado de fraude, manipulación y malversación. Fue puesto en libertad bajo fianza en julio de 2016.

Este es otro de los peores momentos en la historia de Bitcoin. Muchísima gente perdió todo lo que tenía en aquel momento, y se puso de relieve el problema que suponía integrar este nuevo activo en los mecanismos tradicionales.

A partir de este momento, pocos sucesos de interés tienen lugar. Durante 2015 el precio mínimo fue de unos 200 dólares, llegando a superar los 450. En 2016 marcó mínimos de unos 370 dólares, llegando casi a los 1.000 el último día del año.

Cada vez más plataformas aceptan bitcoin como medio de pago, surgen nuevos exchanges y, poco a poco, va siendo conocido por el público general.

Y llegamos a 2017. Aunque para la mayoría de nosotros ha parecido un año frenético, la realidad es que no ha sucedido tanto como parece. Los primeros

años estaban marcados por fallos en el código, las primeras transacciones, el nacimiento de los primeros exchanges, y por una comunidad de fans cada vez mayor. 2017 ha sido el año en que Bitcoin ha pasado a ser mundialmente conocido. El incremento en el precio (desde los 800 a los 19.000 dólares) no ha sido porcentualmente la mayor subida que se ha podido ver en su historia, pero sí ha sido la que le ha puesto en los focos de atención de los medios de comunicación.

Este año fue el nacimiento de Binance, uno de los exchanges más utilizado actualmente. Con tan solo seis meses de vida, consiguió colocarse el número 1 en cuanto a volumen de transacciones. En diciembre se vieron obligados (al igual que Coinbase y varios exchanges más) a cerrar el registro de nuevos usuarios, ya que estaban teniendo problemas con el alto volumen de suscripciones. Tras unos días, al volver a abrir el proceso de registros, se suscribieron a la plataforma más de 240.000 nuevos usuarios en tan solo una hora<sup>[24]</sup>.

### **2.3.6. La bifurcación de la comunidad**

En 2017 tuvo lugar el primer *hard fork* del protocolo de Bitcoin. Un hard fork es una bifurcación contenciosa. Tiene lugar cuando los distintos actores de la comunidad (usuarios, desarrolladores, mineros...) no se ponen de acuerdo en cómo actualizar el código. Cuando surgen estos conflictos, se crean dos blockchains paralelas. Estas dos contienen el mismo pasado común, pero a partir de esa bifurcación cada una se actualiza en función de los nuevos parámetros.

Este conflicto en cuestión se saldó con la creación de Bitcoin Cash. La razón fue la siguiente:

Con la adopción de Bitcoin y el uso cada vez más intenso, las transacciones comenzaron a saturar la red y, por tanto, las comisiones se dispararon. Cuando quieres hacer una transferencia, si pones una comisión mayor, los mineros darán mayor prioridad a tu transacción frente a las demás y tendrá más posibilidad de incluirse en el próximo bloque. Esta situación de congestión estaba provocada por dos factores, el tamaño del bloque (de un megabyte) y el tiempo de minado de 10 minutos. Parte de la comunidad defendía ampliar el tamaño de los bloques a 8 megas y después a 32, mientras que los desarrolladores preferían soluciones de otro tipo para solventar el problema.

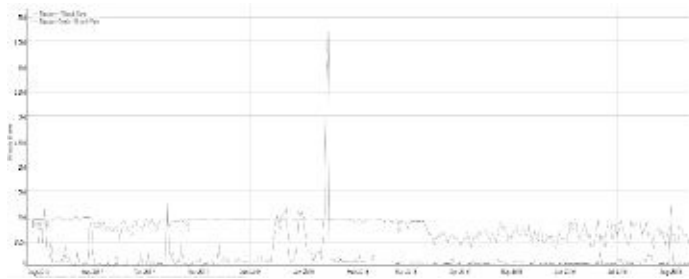
Una de estas soluciones era implementar el Segregated witness. Es un cambio en la estructura de datos del bloque, de tal forma que en la práctica entran más transacciones por bloque. Además, posibilitaba la implantación de soluciones *off-chain* (transacciones que tienen lugar fuera de la blockchain) como Lightning Network. Veremos más adelante en qué consiste.

Este problema del tamaño de los bloques es en parte filosófico. Un tamaño mayor de bloque obliga a que se utilice un hardware más potente y especializado, favoreciendo la centralización. Los principales impulsores de aumentar el tamaño de los bloques eran precisamente los pools de minería.

En cualquier caso, el estado actual de la red no requería aumentar tanto el tamaño de los bloques, y la disputa entre desarrolladores y mineros se saldó con la creación de Bitcoin Cash (BCH).

Esto es lo que ha sucedido desde entonces con el tamaño de los bloques

procesados por ambas cadenas de bloques:



*Fuente: <https://bitinfocharts.com/comparison/size-btc-bch.html>*

Podemos observar cómo el tamaño promedio de BTC ha descendido ligeramente, no llegando al límite, y que los bloques de BCH están muy infrautilizados. El pico que vemos es un test de estrés, en el que los usuarios spamearon miles de transacciones para demostrar que la red no se congestiona. Y es cierto, la red aguantó, pero a pesar de ello por lo general los bloques de BCH están casi vacíos. Si además consideramos la capacidad total de procesamiento de los mineros en la red, llamado *hashrate*, como medida de la salud de una cadena, vemos lo siguiente:



*Fuente: <https://bitinfocharts.com/comparison/hashrate-btc-bch.html#1y>*

Más libros de trading en : <https://t.me/tradingpdfgratis>

En BTC el hashrate aumenta a un ritmo considerable, mientras que el de BCH se ha mantenido constante e incluso ha descendido ligeramente.

Consideramos que este tipo de contingencias van a seguir sucediendo y no es que sea negativo, siempre que haya debate surgirán ideas distintas. Y a veces habrá que llevar las ideas a testearlas al mercado, y ver cuál es la que mejor cumple con las necesidades de los usuarios.

El problema de este tipo de disputas es la imagen que se da hacia el exterior. Alguien que no conozca mucho este ecosistema puede ver que la comunidad está segregada en diferentes corrientes de pensamiento y discutiendo entre sí, y que ello les genere desconfianza.

Este resumen de la historia de Bitcoin es muy breve frente a lo que ha sucedido en realidad, solo pretendemos dar una breve pincelada al lector de lo que ha sucedido desde que un email de un personaje anónimo dio nacimiento a la mayor revolución tecnológica de los últimos años.

## **2.4. Mecanismo de suministro de bitcoins**

Si Bitcoin tiene limitado la cantidad máxima de monedas que habrá a 21 millones, entonces ¿qué ocurrirá una vez que se haya minado la totalidad?, ¿desaparecerá la minería?

Según el protocolo de Satoshi, los mineros recibirían de recompensa por poner sus equipos a trabajar en la red, 50 bitcoins por bloque. Esta cantidad se reduciría a la mitad cada 210.000 bloques (aproximadamente cada cuatro años).

Este hecho recibe el nombre de *halving*. Actualmente en 2018 la recompensa es de 12,5 bitcoins por bloque.

Recordemos que la recompensa por minar un bloque es un incentivo para que:

1. Haya personas dispuestas a poner su equipo a disposición de la red.
2. Compitan entre ellos para ver quién resuelve el bloque antes, es decir, instalen cada vez más capacidad.

Este esquema de suministro no solo es para incentivar a los mineros. Es una forma de distribución de la moneda, ya que no hay una autoridad central que la pueda emitir.

¿Y por qué un suministro limitado? Porque de esta forma, ante un escenario en el que haya adopción a nivel mundial, la moneda será deflacionaria, es decir, con el paso del tiempo debería de valer más. Al crecer la base de usuarios, pero estando la oferta limitada a 21 millones de bitcoins, el precio tenderá a aumentar.

Entonces, ¿qué pasará con los mineros cuando se hayan minado los 21 millones de BTC? ¿Qué incentivo van a tener para seguir proporcionando sus servicios?

Esto es algo que ya tenía pensado Satoshi Nakamoto cuando creó el concepto de Bitcoin. Los mineros serán recompensados solamente con las comisiones de las transacciones<sup>[25]</sup>:

*Una vez que un determinado número de monedas han entrado en circulación, el incentivo puede pasar enteramente a las tarifas de transacciones y estar completamente libre de inflación.*

La forma que tendrán los mineros de ver recompensado su trabajo dependerá totalmente de las comisiones de las transacciones. No olvidemos que

actualmente la recompensa es en la forma de nuevas monedas y en las comisiones de las transacciones incluidas en el bloque.

Para poder ver si finalmente los mineros subsisten solo recibiendo de recompensa las comisiones de las transacciones faltan casi 200 años, ya que se estima que el último bitcoin será minado pasado el año 2200 y, para entonces, ¿quién sabe qué habrá pasado con Bitcoin? ¿Qué tecnología disruptiva existirá en ese momento?

## **2.5. Bitcoin: Burbuja o realidad**

A día de hoy es muy recurrente la pregunta de si Bitcoin es o no una burbuja y si podrá estallar algún día llegando a un valor próximo a los cero dólares.

Es muy fácil encontrar defensores y detractores de la tecnología que tiene detrás y de su posible uso como medio de pago. Por lo tanto, se hace muy complejo poder responder a la pregunta con cierta seguridad.

La única forma que tenemos para darle respuesta es ver qué sucede con el tiempo; de momento nadie puede saber la aceptación que tendrá el Bitcoin en el futuro y si podrá cumplir todas las expectativas con las que nació.

Muchos comparan el gran crecimiento que ha tenido Bitcoin con la burbuja de los tulipanes que tuvo lugar en Holanda en el siglo XVII. En esta gran burbuja, un simple bulbo de tulipán llegó a valer lo mismo que una casa; para que nos hagamos una idea de la magnitud de esta burbuja, algunos bulbos exóticos llegaron a valer más de cien veces la media de ingresos anuales de un holandés.

No es de extrañar que se piense que podemos estar viviendo una burbuja con el Bitcoin y que en algún momento puede estallar, ya que hemos pasado de tener una cotización de apenas céntimos en 2009 a valer 20.000 dólares a finales del 2017.

Pero ¿estamos ante un caso similar al de los tulipanes? Esa burbuja estuvo producida por un momento de especulación colectiva, en el fondo no dejaban de ser tulipanes sin mayor función que la decorativa. Ahora estamos ante una tecnología disruptiva que da solución a un problema. No olvidemos que Bitcoin es un recurso limitado. Solo va a haber 21 millones como máximo. El hecho de tener un activo digital útil y finito es lo que hace que tenga valor. Y los vaivenes en el precio que veremos por el camino son fruto de distintos actores intentando valorar una nueva clase de activo y sus posibilidades reales.

De momento, consideramos que estamos ante una tecnología valiosa que ha llegado para quedarse muchos años con nosotros. La única forma que tendremos de saber si está sobrevalorado es con el paso del tiempo y del nivel de adopción que tenga.

## ■ El ciclo de Satoshi

El ciclo de Satoshi es una forma de relacionar el precio de Bitcoin con las búsquedas que se realizan en internet sobre este activo. El término de ciclo de Satoshi fue acuñado por Chris Burniske<sup>[26]</sup> y lo podemos observar de forma muy clara en el siguiente gráfico:

Más libros de trading en :  
<https://t.me/tradingpdfgratis>



*Fuente: Elaboración propia*

En el primer gráfico tenemos la relación que existe entre las búsquedas en Google con el término Bitcoin y el precio del mismo. Como se puede comprobar, la correlación entre ambas es alta y podemos observar que siguen un patrón similar. Esto tiene una explicación lógica, y es que cuando el precio se incrementa la gente empieza a interesarse más por él y realiza búsquedas para poder invertir y ver las cotizaciones que tiene, esto a su vez ayuda a que entre más capital, suba el precio y el círculo se retroalimenta.

## ■ Manipulación del mercado

El número máximo de bitcoins que puede haber está limitado a 21 millones. Nunca habrá más bitcoins. No solo eso, sino que, además, muchos de ellos se han perdido así que el número total en circulación será bastante menor. Imaginemos la cantidad de gente que puede haber olvidado sus claves, o incluso que hayan enviado bitcoins a una dirección inexistente. Todos esos bitcoins son inaccesibles, y lo seguirán siendo para siempre.

Se piensa que Satoshi Nakamoto, el creador del Bitcoin, posee más de un millón de bitcoins, lo que representaría casi un 5% sobre el total. Con esta gran cantidad de bitcoins se podría alterar el precio en el mercado de forma muy fácil, ya que se podrían inyectar todos estos bitcoins y conseguir que debido al exceso de oferta el precio bajara de forma drástica.

No solo lo podría hacer Satoshi Nakamoto, sino cualquiera que tenga una gran cantidad de ellos. Debido a que los mercados aún no tienen mucha liquidez, el precio se puede alterar de forma drástica con relativa facilidad.

Para hacernos una idea de la capitalización de Bitcoin, vamos a compararla con empresas que todos conocemos. Como curiosidad, el hombre más rico del mundo tenía la misma fortuna que todo el mercado entero de Bitcoin. La fortuna de Jeff Bezos rondaba los 150 mil millones de dólares<sup>[27]</sup>.

En el gráfico siguiente se muestra una comparativa de la capitalización de las empresas más importantes a nivel mundial, del IBEX 35 y del mercado de bitcoins<sup>[28]</sup>.



*Fuente: Elaboración propia*

Como se puede comprobar en el gráfico anterior, Bitcoin capitaliza más que gigantes empresariales como Inditex. Es decir, un activo digital cuya única función es la de intercambio de valor supera a uno de los gigantes textiles más grandes del mundo.

Mientras siga siendo un mercado relativamente pequeño, el precio podrá ser manipulado con relativa facilidad. En cualquier caso, un aumento repentino en las compras o en las ventas puede hacer que el precio oscile salvajemente, como podemos ver habitualmente. Con el paso del tiempo la volatilidad en el precio va disminuyendo, pero queda aún mucho recorrido para que llegue a la estabilidad de las grandes corporaciones o índices bursátiles.

## ■ Cotización del bitcoin

Durante 2017 vivimos un incremento sustancial en el precio del bitcoin. Muchos se han apresurado a decir que ha sido la mayor burbuja que este criptoactivo ha experimentado desde su existencia.

Durante diciembre de 2017 vimos cómo todos los días los grandes medios de comunicación (tanto financieros como generalistas) hablaban como si fueran expertos del tema y explicaban por qué era imposible que cotizara a esos niveles.

Bitcoin es un activo con un suministro limitado, que no está bajo el control de ninguna entidad, y fácilmente transferible. ¿Esto no vale nada? ¿Qué le diferencia del dólar, del euro, o de la rupia? ¿Que no haya un gobierno detrás? ¿Un gobierno que imprime dinero sin control a costa de empobrecer a la población?

A lo largo de la historia el dinero ha ido evolucionando, desde conchas y cristales a monedas de bronce y plata, a cheques y billetes, a apuntes contables digitales como los que tenemos hoy. Pensar que no va a seguir evolucionando es cerrar los ojos a la realidad. Ahora bien, no sabemos qué forma tendrá esa próxima evolución, lo que sí que creemos que tiene sentido es que sea de la manera que nos permiten los criptoactivos.

Tenemos por primera vez un medio de cambio totalmente digital, que no está bajo el control de nadie, que nos permite tener certeza absoluta de que lo que recibimos está exclusivamente en nuestras manos. Y lo podemos intercambiar con personas que estén dispuestas a recibirlo como medio de pago. Tal y como pasa con el dinero tradicional. Hay países que no aceptan un tipo de monedas, pero sí otras. Apostamos a que en muchos lugares se va a preferir el activo digital a la moneda local.

Volviendo al punto anterior, para entender si lo que vimos en diciembre fue una burbuja (o no), primero queremos tener una definición de esta palabra y a continuación reflexionar acerca de lo que hemos vivido. Según Wikipedia:

*Una burbuja económica es un fenómeno que se produce en los mercados, en buena parte debido a la especulación, que se caracteriza por una subida anormal, incontrolada y prolongada del precio de un activo o producto, de forma que dicho precio se aleja cada vez más del valor real o intrínseco del producto. El proceso especulativo lleva a nuevos compradores a comprar con el fin de vender a un precio mayor en el futuro, lo que provoca una espiral de subida continua y alejada de toda base factual. El precio del activo alcanza niveles absurdamente altos*

*hasta que la burbuja acaba estallando, debido al inicio de la venta masiva del activo cuando hay pocos compradores dispuestos a adquirirlo. Esto provoca una caída repentina y brusca de los precios, llevándolo a precios muy bajos, incluso inferiores a su nivel natural, dejando tras de sí un montón de deudas.*

Según esta definición (y casi todas las que hemos encontrado), consideran que una burbuja se produce cuando el valor del activo se aleja de su valor real o intrínseco. Esto es lo importante de la cuestión.

¿Cuánto vale realmente un activo? Estamos hablando de algo totalmente subjetivo.

¿Cuánto vale para nosotros, en nuestra casa, una botella de agua? Posiblemente nada, o unos pocos céntimos en el mejor de los casos.

¿Y si estamos en el desierto?

¿Cuánto vale ahora? ¿Cuál es su valor real?

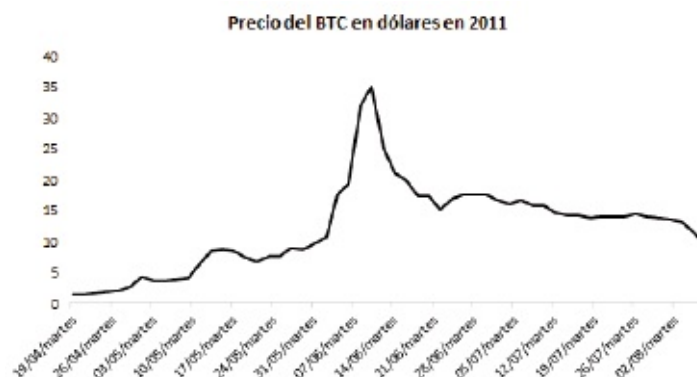
En general, en los mercados, existe consenso en cuál es el precio de las cosas. Pero nunca olvidemos que siempre será subjetivo y que, depende de la situación, estaremos dispuestos a pagar más o menos.

El valor intrínseco de Bitcoin es imposible de averiguar, al igual que es imposible saber el valor intrínseco de un euro. Dependerá de lo útil que sea y de que haya otra persona dispuesta a aceptarlo como medio de pago.

Si has seguido este mundo de cerca ya sabrás que no ha sido la primera vez que Bitcoin multiplica varias veces su valor. Es más, diríamos que es algo habitual en su historia.

Por ejemplo, el 5 de abril del 2011 tenía una cotización de 0,71 \$ y tan solo dos meses más tarde, el 10 de junio, llegó a valor 35 \$. Lo que supone un incremento del 4.829% y, lo más importante, sucedió en un espacio de tiempo muy pequeño. Si comparamos esta rentabilidad con la que dio desde enero de 2017 hasta diciembre, supone más del triple. Y en solo dos meses.

A continuación, tenemos el gráfico con la cotización del precio del bitcoin para mediados del 2011, en él podemos observar el gran incremento de precio que experimentó el bitcoin y como después corrigió:



*Fuente: <https://www.blockchain.com>*

A pesar de dicha corrección, cuando la cotización volvió a bajar, se mantuvo varias veces por encima del precio con el que había iniciado dicho ciclo explosivo. Tal y como ha sucedido durante el 2017 y 2018.

En el siguiente cuadro podemos ver cómo ha variado la cotización en periodos de un año:

**Precio**

**Fin**

**Precio**



| Inicio del periodo | en dólares | del periodo | en dólares | Rentabilidad  |
|--------------------|------------|-------------|------------|---------------|
| 18/08/2010         | 0,07       | 01/01/2011  | 0,3        | <b>305,4%</b> |
| 01/01/2011         | 0,3        | 02/01/2012  | 5,2        | <b>1.650%</b> |
| 02/01/2012         | 5,2        | 02/01/2013  | 13,5       | <b>157,1%</b> |
| 02/01/2013         | 13,5       | 01/01/2014  | 746,9      | <b>543,3%</b> |
| 01/01/2014         | 746,9      | 02/01/2015  | 316,1      | <b>-57,7%</b> |
| 02/01/2015         | 316,1      | 01/01/2016  | 432,3      | <b>36,7%</b>  |
| 01/01/2016         | 432,3      | 01/01/2017  | 997,7      | <b>130,8%</b> |
| 01/01/2017         | 997,7      | 02/01/2018  | 15.005,8   | <b>1.404%</b> |

Todos los años naturales ha experimentado un incremento en su precio a excepción del año 2014. La selección del periodo es totalmente arbitraria y podríamos habernos limitado a estudiar los periodos de mayor incremento.

Pero el mensaje que queremos extraer de aquí es que el bitcoin vale más según pasa el tiempo. Porque cada vez más gente lo conoce y lo utiliza. Hay un valor real que sustenta el precio y es ese.

Puede que no te guste que no lo «controle» nadie. Puede que no confíes en Bitcoin porque es demasiado complejo. Puedes tener mil razones para creer que no vale nada, y pensar que miles de personas se están equivocando (podría pasar, no iba a ser la primera vez que sucede).

Lo que no se puede negar es que es útil. Es útil porque nadie te puede impedir usarlo. Es útil porque puedes recibir y mandar bitcoins sin que nadie pueda censurar la operación. Es útil porque ningún actor puede crear más bitcoins de la

nada y devaluar los que tienes en tu poder. Esto es lo que hace que sea valioso.

¿Cuánto? No sabemos, pero estamos convencidos de que mucho más de lo que vale hoy.

## 2.6. La escalabilidad de Bitcoin

Una de las críticas más habituales que recibe Bitcoin es que no es escalable. Recordemos que cuando hablamos de escalabilidad nos referimos al número de transacciones por segundo (TPS) que permite realizar la red. Actualmente, en promedio, la red procesa alrededor de 3,5 TPS.

Esta es una barrera considerable para la adopción, por lo que los desarrolladores están trabajando en bastantes frentes para poder resolverla. Actualmente la solución conocida como Lightning Network es la que más avanzada está en este campo. Aún está en fase de pruebas, aunque ya se ha lanzado a la Mainnet y es posible realizar transacciones utilizando esta tecnología.

Realizar el cálculo del número de operaciones que soporta la red actualmente es bastante fácil, ya que sabemos que:

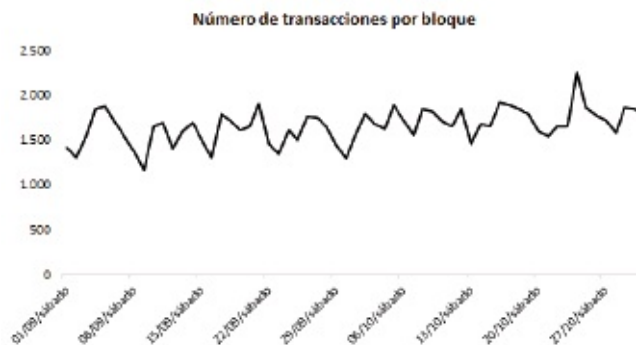
- ▶ El tamaño máximo de cada bloque es de 1 MB o lo que es igual a 1024 kB.
- ▶ El tamaño promedio de cada transacción es de 0,5 kB.
- ▶ Cada bloque de la cadena de bloques se crea cada 10 minutos, es decir, 600 segundos.

Por lo tanto, tenemos que  $\frac{1024 \text{ kB}}{0.5 \text{ kB}} = 2.048$  transacciones por cada bloque de 10

minutos.

Es decir,  $2.048 \text{ transacciones} / 600 \text{ segundos} = 3,41 \text{ transacciones por segundo}$ .

En la imagen de a continuación podemos ver las transacciones que hubo por bloque en los meses de septiembre y octubre del 2018 que, como se puede comprobar, son de una media de unas 1.800 transacciones por bloque.



*Fuente: <https://www.blockchain.com/es/charts/n-transactions-per-block>*

La diferencia de transacciones por cada bloque ocurre porque, aunque el tamaño de bloque no varía, el espacio que ocupan las transacciones sí. En el primer cálculo que se ha hecho para aproximar las transacciones por segundo que había en cada bloque de la blockchain de Bitcoin utilizamos una media de 0,5 kb por transacciones, pero como ya dijimos, es una media, no todas las transacciones son iguales.

Podemos ver con datos reales cómo el número de transacciones por bloque se sitúa por debajo de las 2.000 la mayor parte del tiempo, así que estaríamos hablando de menos de 3,5 transacciones por segundo (recordemos que cada bloque es de 600 segundos, es decir, 2.000 transacciones en 600 segundos son

3,33 transacciones por segundo).

Por tanto, si queremos que Bitcoin sea una moneda de intercambio de valor en el futuro se ha de solventar este problema. Para hacernos una idea, la red de VISA se calcula que realiza unas 1.500-2.000 transacciones por segundo, aunque podría llegar a tolerar por encima de las 45.000<sup>[29]</sup>. Con este dato ya nos damos cuenta de que para que Bitcoin se utilice como un medio de pago masivo hay que aumentar esas 3,33 transacciones por segundo.

Como dijimos anteriormente, el problema de la escalabilidad de Bitcoin es algo que ha preocupado mucho a la comunidad y han salido diferentes alternativas para dar solución a este problema. La que parece más asentada y que más gusta es la de Lightning Network que, resumiendo mucho su explicación, es una red de pagos atómicos (los pagos se realizan o no, pero no pueden quedar en un limbo entre los dos estados) que permite realizar pagos y micropagos de forma instantánea sin necesidad de delegar la custodia de los fondos a un tercero de confianza como podría ser un banco.

La solución de Lightning Network propone crear canales de pago o *payment channels* que estén *offchain*, es decir, fuera de la blockchain, donde el envío y recepción de fondos se hace mediante compromisos de pagos. Con esta solución se consigue que las transacciones sean instantáneas y se reduce así la saturación de la cadena de bloques.

A continuación, os explicaremos más a fondo cómo funciona y cómo da solución a estos problemas.

Por ahora, recordemos que hacer una transacción con Bitcoin tiene asociado una comisión que va a los mineros; si queremos hacer una transacción muy pequeña

de dinero podría darse el caso de que para que los mineros verificaran esa transacción tuviéramos que pagar más dinero de comisiones que el propio valor de la transacción. Esto, obviamente, no tiene ningún sentido.

Dependiendo de lo saturada que esté la red de Bitcoin, las comisiones de las transacciones que se incluyen en la cadena de bloques varían. En el último trimestre de 2018, la comisión por hacer una transacción está entre los 0,35-0,55 dólares. Tenemos que recordar que en diciembre de 2017 algunos días se llegó a pagar más de 50 dólares por cada transacción<sup>[30]</sup>. No tiene sentido pagar una comisión tan elevada si queremos comprar un producto de escaso valor.

Ahora que estamos en contexto, vamos a empezar con el funcionamiento de los canales de pago para más adelante explicaros cómo funciona la red de Lightning Network, que está basada en estos canales pago.

Pensemos en dos personas que continuamente están haciendo transacciones entre ellas. A lo largo del día pueden tener decenas de operaciones. Estas dos personas o entidades (que podría ser una empresa y un proveedor, un cliente con un bar, un cliente en un supermercado...) crearían una dirección multifirma 2 de 2 donde enviarían una transacción inicial con los fondos que van a poner cada una en el canal. Una dirección multifirma 2 de 2 quiere decir que para poder realizar transacciones desde esa dirección hacia otras se necesita la firma (clave privada) de los dos participantes, así se tienen que poner de acuerdo ambas partes para poder hacer cualquier transferencia de valor desde esa dirección.

Para abrir el canal, no es necesario que ambas partes pongan fondos, ya que, por ejemplo, en un canal de pagos con un restaurante no tendría sentido que el restaurante pusiera fondos para abrir un canal con un cliente, en cambio, entre

dos amigos sí podría tener sentido que ambos pusieran fondos para un canal, ya que podrían dejarse dinero mutuamente o realizarse pagos por servicios.

Esta primera transacción de fondos que iría a la dirección multifirma que han creado y se registraría en la blockchain para poder abrir el canal de pago entre las dos partes. A continuación, una vez que el canal está abierto, ya se pueden enviar fondos el uno al otro mediante transacciones que son llamadas transacciones de compromiso, es decir, se hacen compromisos de pagos entre las partes que una vez que se cierre el canal se llevará el resultado a la blockchain.

Imaginemos que Alicia abre un canal de pagos con Bruno, y que cada uno de ellos deposita 1 bitcoin, es decir, la primera transacción de fondos que se registra en la blockchain es de 2 bitcoins (uno de Alicia y otro de Bruno).

Ahora imaginemos lo siguiente, fuera de la red blockchain, en el canal de pagos que tienen abierto Alicia y Bruno, se empiezan a realizar transacciones entre ellos:

- ▶ Alicia hace un pago a Bruno por 0,2 bitcoins.
- ▶ Bruno hace un pago a Alicia por 0,3 bitcoins.
- ▶ Bruno hace un nuevo pago a Alicia de 0,1 bitcoins.
- ▶ Bruno hace otro pago más a Alicia de 0,1 bitcoins.

Al principio, cada uno tenía 1 bitcoin en su poder, pero ahora después de haber realizado diferentes transacciones de compromiso en el canal de pago, el saldo para cada uno sería:

$$\diamond \text{ Alicia} = 1 - 0,2 + 0,3 + 0,1 + 0,1 = 1,3 \text{ bitcoins}$$

◇ Bruno =  $1 + 0,2 - 0,3 - 0,1 - 0,1 = 0,7$  bitcoins

Si ahora decidieran cerrar el canal, se llevaría a la blockchain el saldo de las cuentas para registrar que Alicia ahora dispone de 1,3 bitcoins y Bruno ahora dispone de 0,7 bitcoins.

Los canales de pago pueden permanecer abiertos el tiempo que acuerden las partes que lo abren, y solo se registran los saldos del canal cuando este es cerrado.

En vez de llevar todas las transacciones contra la blockchain y pagar comisiones por cada una de ellas, solo se lleva la creación y el cierre del canal de pagos, por lo tanto, se reduce la saturación de la red y se evita que debido a esta las comisiones en la cadena de bloques aumenten de forma descontrolada, como pasó en diciembre del 2017.

Para realizar las transacciones de compromiso entre las partes, se intercambian transacciones firmadas por el emisor con el nuevo saldo que tendrían las cuentas. Recordemos que al principio habíamos abierto una cartera multifirma 2 de 2, es decir, que para que se realice esta transacción y se propague a la red de blockchain el resultado de las cuentas tendría que ser firmada por el receptor. Cada vez que se hace una transacción, está reflejado el nuevo saldo que tendrían las cuentas y la firma del emisor. Esto se hace así para que el receptor pueda cerrar el canal si quiere después de recibir esa transacción y reflejar en la blockchain el saldo final de las cuentas. En caso de que no quiera cerrar el canal, en la siguiente transacción se tendrá en cuenta el saldo de cada uno.

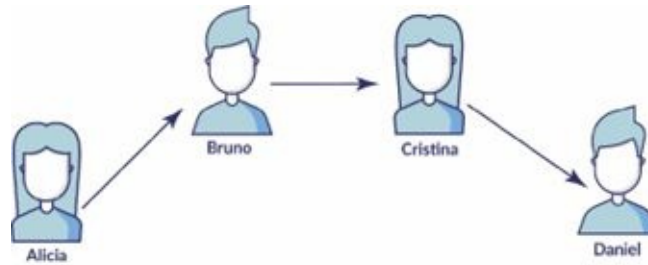
Lógicamente, si ambas partes tienen todas las transacciones de compromiso firmadas por la otra parte, podría darse el caso de que alguna de las dos intentara

tomar ventaja y firmar una transacción más ventajosa para sí mismo, cerrando el canal y propagando ese resultado de fondos a la blockchain. Para combatir esto las transacciones se pueden hacer revocables; de esta forma, el que cierra el canal tendría que esperar un tiempo<sup>[31]</sup> para poder sacar los fondos de la cartera multifirma 2 de 2. Durante este tiempo la otra parte podría reclamar que el estado propagado a la red no es el correcto y que el estado de las cuentas en el canal de pagos era diferente; si esto ocurre, la parte deshonesto podría ser penalizada con la pérdida de los fondos del canal.

Ahora que hemos explicado cómo funciona un canal de pagos, vamos a ver cómo funciona la red de Lightning Network.

Esta red se forma cuando hay varios canales de pagos entre diferentes usuarios que tienen algún otro usuario en común. Se basa en utilizar canales ya formados por otros usuarios para poder realizar transacciones con usuarios que están fuera de nuestra red sin necesidad de abrir un canal nuevo.

Por ejemplo, Alicia abre un canal de pagos con su compañero de trabajo Bruno y, a su vez, Bruno ya tenía abierto un canal de pagos con su amiga Cristina y esta, a su vez, con su novio Daniel. Si Alicia quisiera enviar dinero a Daniel por un regalo que compró para el cumpleaños de Bruno, tendría dos opciones, podría abrir un canal de pagos directamente con Daniel para transferirle el dinero, o aprovecharse del potencial de Lightning Network y usar la red que ya está creada con Bruno y con Cristina para hacerle llegar los fondos.

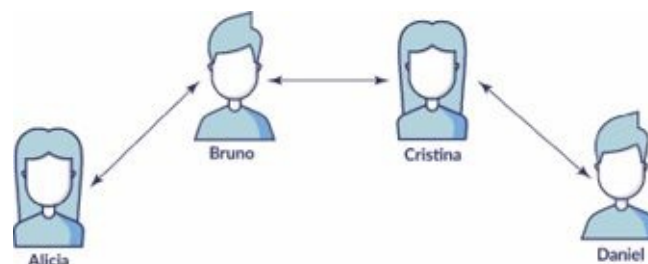


Para hacer llegar los fondos desde Alicia hasta Daniel, se utilizan contratos de tipo HTLC<sup>[32]</sup> (Hash TimeLock Contract).

Por no entrar en detalles demasiado técnicos, el receptor de los fondos tendrá que reconocer mediante su firma que ha recibido los fondos, o estos serían devueltos al pagador tras un periodo de tiempo.

Vamos a intentar entender Lightning Network con el ejemplo anterior:

1. Alicia tiene un canal abierto con Bruno, este a su vez tiene abierto uno con Cristina y esta a su vez tiene abierto uno con Daniel. Es decir, tenemos cuatro intervinientes en esta red de Lightning Network con tres canales de pago, el de Alicia-Bruno, Bruno-Cristina y Cristina-Daniel.

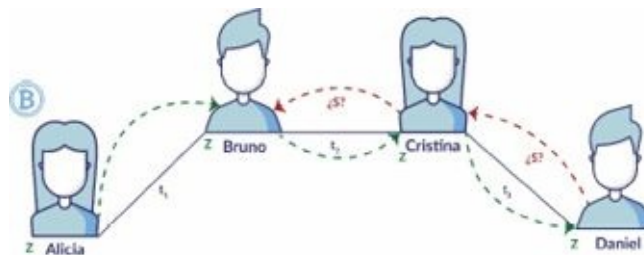


Si Alicia quiere enviar fondos a Daniel, lo primero que tiene que hacer es avisarle de que le quiere hacer un envío de fondos. En ese momento, Daniel crea un valor secreto que llamaremos  $S$  y le aplica la función *hash* convirtiéndolo en  $Z$ . Una vez que tiene  $Z$ , pasa este valor a Alicia.

►  $Z = \text{Hash}(S)$

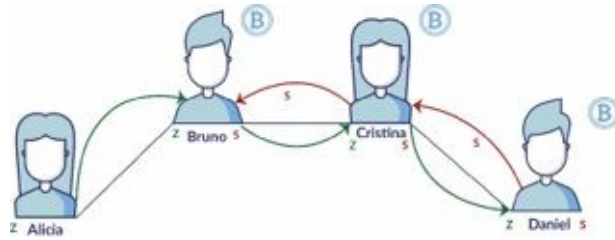
2. El segundo paso es que Alicia y Bruno hagan un contrato HTLC, donde Alicia se comprometa a pagar una comisión a Bruno si este puede generar la solución de Z en menos de un tiempo que llamaremos  $t_1$ . A continuación, Bruno hará un contrato similar con Cristina, pero reduciendo el tiempo para conseguir generara la solución de Z ( $t_2$ ) y Cristina hará lo mismo con Daniel, pero con un tiempo aún menor ( $t_3$ ).

►  $t_1 > t_2 > t_3$



3. Una vez que la red se ha completado y que Daniel tiene un contrato con Cristina, este puede cobrar los fondos de Cristina a cambio de darle solución de S, con lo que podría dar como finalizado el pago de Alicia. A su vez, Cristina dará la solución a Bruno y recibirá el pago, y Bruno dará la solución a Alicia y recibirá el pago.

De forma resumida, una vez que Daniel de la solución de S a Cristina se suceden una serie de pagos en cadena entre los cuatro intervinientes de la red y el resultado es que los fondos llegan desde Alicia hasta Daniel a través de los diferentes contratos que han abierto entre ellos.



En el ejemplo anterior teníamos a cuatro intervinientes que hemos supuesto que eran personas, pero si imaginamos que, por ejemplo, Bruno y Cristina son dos empresas grandes como Amazon o Netflix, con muchos canales de pagos con clientes, podremos hacernos una idea del potencial que puede llegar a tener esta tecnología si finalmente se adopta en el futuro.

Podríamos enviar dinero a multitud de personas sin necesitar crear un canal de pagos con ellos, aprovechándonos de los canales creados por otros usuarios o grandes empresas.

## Conclusión

Al llegar a este punto, esperamos que el lector empiece a entender un poco lo que significa Bitcoin. Lo que conocemos como blockchain existe gracias a Satoshi Nakamoto y a la prueba de trabajo que, por primera vez, soluciona de forma efectiva los problemas de confianza en redes de ordenadores distribuidas.

Pero aparte de la revolución tecnológica que supone, también es una revolución del sistema financiero. Por fin existe un nuevo tipo de activo que permite ser utilizado como dinero, pero sin estar bajo el control de nadie. Y su precio podrá subir o bajar, pero ningún actor puede «imprimir» más billetes a su antojo. Nadie está en el poder. Todos somos iguales en una economía basada en Bitcoin.

### 3. Blockchain

Como ya hemos visto, Bitcoin es un ejemplo de aplicación de tecnología blockchain. Blockchain es un software, por lo que se puede adaptar de mil maneras a las necesidades de cada persona o empresa.

Por lo general, no existe un consenso en las definiciones más básicas, por lo que expresaremos nuestra forma de entender la tecnología en este momento de la forma más genérica posible. Queremos que el lector sea consciente de que puede encontrar definiciones distintas, y ser estas igual de válidas.

Para explicar la tecnología blockchain, seguiremos utilizando el ejemplo de Bitcoin. ¿Por qué? Porque todo cambia de una blockchain a otra, y sería muy incómodo y poco intuitivo poder seguir el hilo si habláramos de diferentes blockchains a la vez.

El funcionamiento de la blockchain de Bitcoin de forma muy simplificado sería el siguiente:

1. Un usuario realiza una transacción.
2. Esta transacción se verifica criptográficamente para asegurar que está enviando un activo digital que está en su poder.
3. Se agregan transacciones en un bloque hasta ocupar el espacio disponible.
4. Este bloque vuelve a ser verificado criptográficamente, comprobándose que las transacciones se ajustan al protocolo de la red. De ser así, es validado y se une al bloque anterior, formando una cadena.

5. Una vez forma parte de la cadena, no se puede eliminar ni alterar el contenido.

Es decir, un usuario transfiere un activo digital a otro. Cuando un usuario hace una transacción, el activo deja de estar en su poder y pasa a estar en poder del receptor. Esto sucede de forma confiable gracias a la criptografía y, además, no se puede gastar la misma moneda dos veces, ni cancelar un envío realizado.

### **3.1. Transacciones**

Una blockchain es básicamente un libro de contabilidad. Una transacción consiste en una salida de un activo digital de una cuenta (o cartera), y en la entrada en otra.

Ahora que tenemos el esquema más claro en la cabeza, vamos a complicarlo un poco:

Una cartera es una dirección en la blockchain, donde se encuentra alojado el criptoactivo nativo de la red. Esos activos solo pueden ser movidos mediante una firma digital, que se hace a través de la clave privada que solo deberá conocer el propietario (y que debe de guardar de forma segura, ya que, si la extravía o se la roban, sus fondos se pierden).

Utilizando el ejemplo de Alicia y Bruno:

- ▶ Alicia quiere enviar a Bruno un bitcoin.
- ▶ Accede a su cartera, comprueba que tiene fondos suficientes, y empieza la

transacción. Para que esta se pueda realizar, tendrá que autorizarla mediante su clave privada. Esta clave permite acceder a los fondos, y firmar la transacción. En la transacción lo que realmente sucede es que Alicia está firmando un mensaje que dice que el nuevo propietario de los fondos es Bruno.

- A partir de este momento solo tendrán que esperar a que la operación sea minada y Bruno verá el bitcoin en su cartera.

## 3.2. Bloques

Un bloque es un conjunto de transacciones firmadas digitalmente, con un sello de tiempo y con la huella digital del bloque anterior.

La estructura de un bloque consiste en tres partes:

◇ **Cabecera:** En ella aparecen una serie de metadatos.

- El primer dato es el hash anterior, para identificar el bloque precedente. Es la huella digital que acabamos de mencionar (explicamos unos párrafos más adelante qué es el hash).
- Dificultad: La dificultad es un parámetro variable en función de la cantidad de capacidad computacional que hay en la red. Aumenta o disminuye para que el tiempo promedio en resolver un bloque sea de 10 minutos. Para resolver un bloque, el minero tiene que devolver un hash menor al valor límite que marca la dificultad. Por explicarlo de forma sencilla, la

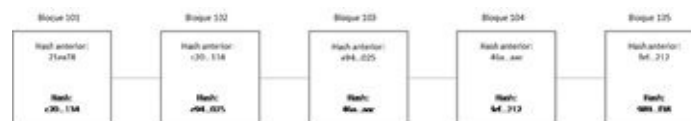
dificultad da un número que comienza por muchos ceros. Cuantos más ceros haya, más difícil sería resolver el problema. El minero tiene que probar combinaciones numéricas con el contenido de un bloque hasta que un resultado dé un número por debajo del valor de la dificultad.

- ▶ Sello de tiempo o timestamp: Sirve para asegurar que la cadena discurre en orden cronológico correcto.
  - ▶ *Nonce*: Viene de «Number that can only be used Once», es un valor aleatorio de 32 bits que se combina con el hash como medida de seguridad para impedir que se altere la información contenida en el bloque. Este valor aleatorio es el que intentan descubrir los mineros, probando todas las combinaciones posibles hasta que una de ellas dé un hash menor al de la dificultad objetivo del bloque.
- ◇ **La información:** Como ya hemos comentado, un bloque contiene toda la información acerca de las transacciones realizadas, es decir, quién envía, quién recibe, y la cantidad.
- ◇ **El hash:** Es el resultado de una función criptográfica que, independientemente de la longitud de unos datos de entrada, devuelve una serie alfanumérica de una longitud determinada. Actúa como una huella dactilar, y cada bloque tiene un hash único. Una vez que se crea un bloque, el hash resultante es producto de toda la información que contiene. Si alguien modifica cualquier dato que el bloque contenía, el hash será distinto y, por tanto, se sabrá que el registro ha sido alterado.

Vamos a explicar un poco mejor la parte de la dificultad:

El algoritmo de Bitcoin tiene establecido que se resuelva un bloque cada 10 minutos (en promedio). El ejercicio de minar (resolver un bloque) es probar combinaciones numéricas aleatorias con el contenido del bloque. No se puede saber de antemano cuál es la combinación correcta hasta que una de estas combinaciones devuelva un resultado menor al marcado por la dificultad, pues el tiempo que se tarda en resolver el bloque estará en función de cuánta capacidad de cálculo haya en la red, es decir, cuántos mineros estén a la vez intentando dar con la combinación. Si hay más mineros, cada vez tardarían menos en resolver este acertijo. Para evitar que el tiempo promedio baje (o suba), existe lo que conocemos como la dificultad. Es una función que recalcula cada 2.016 bloques la velocidad con la que se están resolviendo, y sube o baja para mantener el tiempo promedio objetivo que, como dijimos anteriormente, es de unos 10 minutos.

Veamos un ejemplo de una blockchain y qué pasa si alteramos el contenido:



Cada bloque tiene en su cabecera el hash del bloque anterior, y en la parte inferior el hash resultado de la función criptográfica aplicada sobre la información que contiene el bloque. Podemos ver que el campo «hash anterior» siempre coincide con el campo «hash» del bloque previo en la cadena.

Ahora veamos qué sucede si modificamos la información contenida en el segundo bloque:



Aunque hayamos cambiado un solo punto en toda la información que contenía el bloque 2, el hash resultante es completamente distinto. Como consecuencia de esta manipulación, todos los bloques posteriores ahora se invalidarán porque ya no almacenan el hash anterior correcto. Lo que está sucediendo en este ejemplo es que la cadena de repente se ha roto y todos los bloques posteriores a la manipulación serían inválidos y habría que recalcularlos.

Un atacante podría alterar un bloque de la cadena para introducir operaciones irregulares, y volver a recalcular el hash de todos los bloques posteriores para que la cadena parezca inalterada y legítima. Ahí es donde entra en juego el algoritmo de la prueba de trabajo que os contaremos más adelante. Este atacante tendría que ser capaz de recalcular toda la blockchain posterior, e ir añadiendo nuevos bloques, más rápido que todos los mineros honestos. Es por esto por lo que en la práctica es casi imposible alterar un bloque que ya forme parte de la cadena.

### 3.3. Algoritmos de consenso

El consenso es una forma de llegar a un acuerdo en grupo. Las blockchains, al ser descentralizadas, requieren que los participantes decidan y acepten qué eventos han tenido lugar de forma que se ajusten al protocolo y validarlas. El consenso es lo que permite que la mayoría acepte una propuesta y que no haya disputas. Esto es necesario porque recordemos que estamos interactuando en un

sistema donde potencialmente hay actores deshonestos y no sabemos quiénes son.

Ahora bien, el problema de cómo alcanzar consenso en una red donde puede haber actores maliciosos es una variante del problema de los generales bizantinos<sup>[33]</sup>. Se plantea de la siguiente forma:

Una serie de generales del ejército bizantino están acampados en las afueras de una ciudad. Entre ellos solo se pueden comunicar mediante mensajero, y tienen que observar al enemigo para decidir un plan de acción. Algunos de estos generales podrían tratarse de traidores, por lo que pueden intentar prevenir que los demás alcancen un consenso. Por ello necesitan un algoritmo que les permita:

1. Que los generales leales hagan lo que les diga el algoritmo (los traidores harán lo que quieran). Y el algoritmo tiene que garantizar esta condición independientemente del comportamiento de los traidores.
2. Un número pequeño de los traidores no puede provocar que un general leal adopte un plan distinto al que adopten los demás generales leales.

Explicado de una forma más simple, múltiples actores, desconocidos entre sí, y separados físicamente, tienen que ponerse de acuerdo en unos hechos antes de tomar una decisión. Esto se logra mediante un sistema que hace que los actores honestos actúen siempre mediante las reglas establecidas independientemente de lo que hagan los actores maliciosos.

Satoshi Nakamoto, creador de Bitcoin, solucionó este problema mediante la prueba de trabajo<sup>[34]</sup>. De cualquier modo, existen distintas formas de alcanzar

este consenso, y cada blockchain puede utilizar un mecanismo diferente, ya que tienen distintas implicaciones.

### ***3.3.1. Prueba de trabajo o Proof of work (PoW):***

En una blockchain, tiene que existir un mecanismo para decidir qué hechos han sucedido, y de forma consensuada, aceptar esos hechos y añadirlos a la cadena de bloques. Uno de los mecanismos de consenso más habitual es el de prueba de trabajo o *proof of work (PoW)*.

En un sistema PoW como Bitcoin o Ethereum, los nodos (llamados mineros) compiten entre sí para resolver una prueba criptográfica. Sería como intentar resolver un acertijo matemático extremadamente complejo. Solo existe una forma de resolver este acertijo: probar combinaciones numéricas una a una hasta que la respuesta dada por el algoritmo cumple con los parámetros necesarios (marcados por la dificultad de la red).

El primer nodo que lo consiga recibe como recompensa nuevas monedas y las comisiones de las transacciones incluidas en el bloque. El resto de nodos de la red comprobará que la solución propuesta por este minero es correcta. De no serlo, la mayoría de los nodos en la red lo descartarán y, por tanto, al no haber consenso, los mineros no trabajarían sobre esa cadena.

Los mineros hacen lo siguiente:

- ◇ Agregan en un bloque las transacciones que están en un *pool* esperando. Las operaciones, hasta que no sean añadidas a la cadena, no tienen efecto.

- ◇ Para poder añadir el bloque a la cadena, tienen que encontrar un número aleatorio (nonce) que, aplicado sobre el contenido de todo el bloque, devuelva un hash (resultado de la función criptográfica) menor al valor límite establecido por la dificultad de la red.
- ◇ El minero que encuentra ese nonce valida el bloque y el resto de mineros comprueba que la solución alcanzada satisface las condiciones del protocolo. El minero que ha validado el bloque recibe una recompensa en forma de:
  - ▶ Nuevas monedas.
  - ▶ Comisiones de las transacciones del bloque.

Estas recompensas tienen el objetivo de incentivar la entrada de más mineros a la red, aumentar la competencia y, por tanto, hacer más segura la red. Cuantos más mineros haya en la red, más difícil es que un actor malicioso pueda atacarla.

## ■ Ataque del 51%

Vamos a hacer un pequeño inciso para explicar qué es un ataque del 51%:

Se llaman ataques de consenso o del 51% porque en un sistema proof of work, si un ente controla más del 50% de la capacidad computacional o hashrate de la red, teóricamente tendría capacidad para realizar operaciones de doble gasto.

Este doble gasto consiste en lo siguiente: El atacante realiza una transacción válida, firmada con su clave privada. La operación pasa a un pool esperando a ser minada. Una vez que ha sido minada, y se han añadido seis bloques, el receptor de la transacción tiene certeza de que la operación es válida. Se dice que tras seis bloques la transacción está confirmada porque hay menos de un 0,1% de

probabilidad de que finalmente esta cadena se rechace y se siga minando en otra cadena diferente.

Mientras tanto, el atacante ha creado una bifurcación de la blockchain donde esa transacción aún no había tenido lugar. Vuelve a enviar a otra persona esos bitcoins, y se pone a minar con toda la capacidad de cálculo en esta segunda cadena. Al tener más capacidad computacional que el resto de la red, en teoría esta cadena terminará siendo más larga y, por tanto, será la aceptada por la mayoría de participantes. Cuando hay dos cadenas a la vez se convierte en una carrera. Ganará la que más bloques agregue. Al tener más capacidad computacional una de las dos cadenas tenderá a crecer ligeramente más rápido que la otra y será la aceptada. Tenemos que recordar que, aunque la dificultad de minado varíe en función de la capacidad de computación total de la red, esta se recalcula cada 2.016 bloques (en Bitcoin). Las dos cadenas tendrán la misma dificultad de minado, pero una de ellas será finalmente más larga por tener mayor capacidad de cálculo trabajando sobre ella.

¿Vemos qué conlleva esto?

Puedo pagar dos veces con el mismo bitcoin, y uno de los dos receptores verá cómo ese bitcoin desaparece de su cuenta cuando la cadena alterada se imponga como la cadena válida. No quiere decir que pueda crear monedas de la nada, simplemente que puedo enviar una cantidad que tenga en mi cuenta a distintas personas.

Imaginemos que contrato a dos profesionales que aceptan bitcoins como pago. A uno le encargo un plan de marketing y al otro todo el diseño gráfico. Hago la transferencia del pago acordado a los dos, y recibo el trabajo contratado. Dentro

de un tiempo, a uno de ellos le faltará ese bitcoin de su cartera, aunque previamente lo haya visto. Por tanto, he pagado a ambos con la misma moneda, y finalmente una de las dos desaparecerá.

Hasta ahora Bitcoin nunca ha sufrido este tipo de ataques, pero otras cadenas con menos hashrate sí. El hashrate recordemos que es la capacidad computacional total de la red, y si es suficientemente baja, podríamos contratar la potencia necesaria en servidores para realizar un ataque satisfactorio.

Respecto a la seguridad, los mineros son un elemento crucial. Cuantos más haya y más distribuidos estén a lo largo y ancho del mundo, más segura será la red porque habrá menor riesgo de que un actor malicioso sea capaz de sumar el 51% de la capacidad total de procesamiento. Su función, como hemos dicho, es la de agregar las operaciones en bloques y validarlos. Y como todo esto tiene unos costes (en equipo y en electricidad), se les retribuye por ello. En concreto, en Bitcoin, cada vez que un bloque es añadido a la blockchain, el minero que lo ha hecho recibe una recompensa en forma de nuevos bitcoins, actualmente 12,5 bitcoins por bloque resuelto. Adicionalmente, ganan las comisiones que llevan asociadas las transacciones.

## ■ Comisiones

Las comisiones cumplen varias funciones. Por un lado, mantener una infraestructura de blockchain es costoso y hay que pagar a aquellos que estén dispuestos a contribuir dedicando sus recursos. Los mineros, aparte de la recompensa en forma de nuevas monedas, se llevan las comisiones asociadas a las transacciones. Recordemos que, en Bitcoin, cada 210.000 bloques la

recompensa se reduce a la mitad. Pero no es la única razón por la que existen comisiones. Cada vez que alguien desea hacer una transacción, todos los participantes de la red tienen que procesar esa operación. Un actor malicioso podría intentar bloquear la red mediante un ataque tipo spam, es decir, generar millones de operaciones vacías con el fin de saturar los bloques y que las transacciones tarden más en procesarse. Para evitar este ataque, todas las transacciones llevan una comisión variable, que se puede modificar en función de la urgencia que se tenga porque se confirme y de la congestión de la red. Los mineros darán prioridad para incluir en los bloques las operaciones que tengan comisiones más altas.

Esto, a pesar de que es un mecanismo para evitar congestionar la red, puede convertirse en un incentivo perverso. Si los mineros deciden no incluir en los bloques las transacciones que estén por debajo de una comisión, podrían unilateralmente imponer unas condiciones al mercado.

Pero no todas las blockchains tienen comisiones, existen, por ejemplo, blockchains que utilizan mecanismos diferentes para incentivar y protegerse de los ataques sin necesidad de tener comisiones.

Por ejemplo, en EOS, los validadores reciben de recompensa nuevas monedas. No hay comisiones en las transacciones. Con este planteamiento, los que tienen monedas sufren una lenta erosión en su poder adquisitivo, y pagan por el mantenimiento de la red, hagan uso de ella o no.

Otras monedas como Nano se protegen contra los ataques spam obligando a resolver una PoW sencilla cuando se quiere ejecutar una transacción. De esta forma, un atacante no puede realizar varios miles de millones de operaciones instantáneamente, ya que cada envío conlleva varios segundos de procesamiento.

Necesitaría actuar con cientos o miles de equipos en paralelo con los costes que eso conlleva.

## ■ Características de Bitcoin

A partir de la creación de Bitcoin, y con el paso de los años, han ido surgiendo otras criptomonedas basadas en la tecnología blockchain y se han desarrollado casos de uso distintos más allá de la transacción financiera.

La blockchain de Bitcoin presenta estas características:

- ▶ Pública: Cualquiera puede participar en la red y abandonarla libremente.
- ▶ Distribuida: Todos los participantes mantienen una copia del mismo registro.
- ▶ Descentralizada: Nadie tiene poder sobre los demás, no hay una entidad que gestione Bitcoin, ni que pueda «apagar» o cerrar la red.
- ▶ Su mecanismo para añadir bloques a la cadena es la prueba de trabajo, que requiere de mineros cuya capacidad de cálculo agregada da robustez a la red.
- ▶ Inmutable: Un bloque que forma parte de la blockchain no puede ser alterado sin modificar todos los registros posteriores, lo que generaría el rechazo por parte de los demás participantes de la red.

Por tanto, la blockchain de Bitcoin es pública, distribuida y descentralizada, y utiliza el algoritmo de prueba de trabajo para validar bloques. Cada proyecto de blockchain, al final, es ligeramente distinto dependiendo de cómo juegue con estas características, pero el punto común a todas es que son inmutables.

En cuanto al anonimato, las transacciones que suceden en la blockchain son

visibles para todo el mundo. Podemos ver el recorrido de todos los bitcoins hasta su origen, y saber por qué cuentas han pasado.

¡Esto no significa que sepamos a quién pertenecen! Aunque hay un pequeño matiz.

Cuando abrimos una cartera de Bitcoin (una *wallet*, que simplemente es una dirección de la blockchain que solo nosotros podemos desbloquear) no proporcionamos ningún dato personal. Nadie sabrá que es nuestra, ni hay una base central donde se almacene información acerca de nosotros. Aunque, eso sí, en el momento en que la utilizemos para que nos envíen fondos (o nosotros se los enviemos a alguien) esa persona podrá atar cabos, ver nuestros movimientos y saber el saldo de la cartera.

## ■ Descentralización y minería

Recordemos que minar es una competición. Quien antes resuelva un bloque, se queda con las nuevas monedas creadas y las comisiones. Al ser una lucha por ser el primero, todos los participantes van a intentar ser lo más competitivos posibles en los costes de electricidad y hardware.

Hay ciertos argumentos defendiendo que mediante este modelo se tiende a la centralización, ya que se provoca que solo los participantes más fuertes puedan competir. Las ventajas que pueden tener unos actores frente a otros son:

1. Tener acceso a capital más barato: Si pago menos intereses por mi deuda, más fácil será que gane dinero con la actividad y tengo más margen para reinvertir en comprar más equipos de minería.

2. Menores costes de electricidad, mano de obra y mantenimiento: No es lo mismo pagar la luz en un domicilio, que contratar con una empresa eléctrica el equivalente a 100 o 1.000 hogares. Hay países en los que minar no es rentable solo por el coste eléctrico, mientras que en otros la electricidad es prácticamente gratis.
3. Acceso directo a fabricantes de hardware: De igual forma, si voy a una tienda de componentes y compro cuatro equipos para minar, no voy a obtener ningún descuento. Pero ¿y si tengo la posibilidad de negociar miles de equipos directamente con un fabricante?

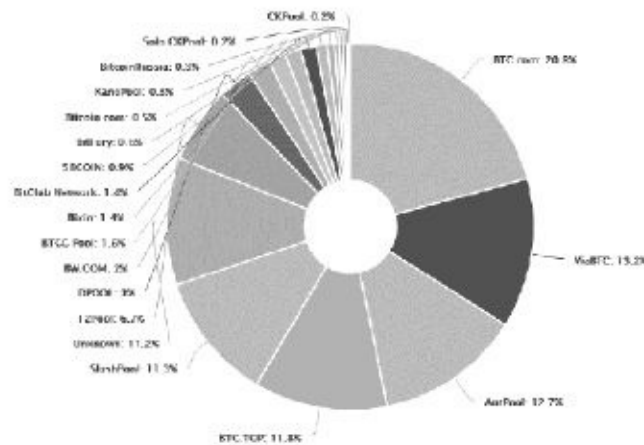
Ya vemos por dónde va el argumento, ¿verdad? En una competición a nivel mundial, solo podrá mantenerse en la carrera aquel que apenas pague electricidad, que además pueda negociar con fabricantes, y que le cueste muy poco financiarse.

Esto lleva a la centralización.

Existen dos formas de tender hacia la centralización. O a través de los pools de minería o a través de las empresas manufactureras.

Un pool de minado tiene como función agregar la potencia de cálculo de varios mineros con el fin de resolver un bloque, y repartir la recompensa entre ellos. Hoy sería imposible comprarse un equipo de minado y tratar de competir contra toda la red para resolver un bloque, recordemos que gana quien resuelva una operación criptográfica cuya solución es aleatoria. Por tanto, quien más combinaciones posibles prueba, más probabilidad tiene de ganar.

Esta tendencia a agruparse en pools lleva a una centralización, como podemos ver en la siguiente imagen:



En agosto de 2018, los cinco principales pools de Bitcoin acaparan casi el 70% del hashrate total de la red. Esto quiere decir que, en caso de que se produjera un pacto entre ellos, tendrían control total sobre las transacciones que se efectúan.

En el caso de Bitcoin, primero se minaba con CPU, es decir que cualquier persona con un ordenador en casa podía minar. Después se pasó a minar con tarjetas gráficas (*Graphic Processing Unit* o *GPU*), que ya requerían un poco más de sofisticación y de gasto económico.

En cuanto a las blockchain PoW que se minan con tarjetas gráficas, la imagen no es mucho mejor. Prácticamente toda la producción se la reparten entre AMD y Nvidia.

¿Existe descentralización cuando todo el hardware lo producen tan pocos actores?

¿Qué pasaría si introdujeran un software que les permitiera controlar el equipo remotamente? ¿O dejarlo totalmente obsoleto?

Algunos protocolos han hecho modificaciones al algoritmo para que sea «resistente» a los ASIC, y así luchar contra la centralización de este tipo. Pero no nos equivoquemos, no hay ningún algoritmo que pueda resistir la creación de un equipo altamente especializado. Solo hace falta tiempo y dinero para que se pueda diseñar un ASIC para cualquier algoritmo. La única forma de luchar contra esto es cambiando regularmente el algoritmo para que cada vez que salga un nuevo modelo de ASIC, se quede obsoleto.

Esto es lo que hicieron los desarrolladores de Monero cuando una empresa anunció que iban a sacar a la venta los primeros equipos ASIC para esta criptomoneda. Tras realizar el cambio de algoritmo que dejaría obsoletos a estos equipos, el hashrate cayó un 80%. Es decir, ya había ASIC minando de forma secreta.

### ***3.3.2. Prueba de participación (Proof of Stake o PoS)***

Este sistema de consenso funciona de forma muy distinta al PoW. El usuario,

para tener el derecho de validar bloques, tiene que tener unos fondos en la criptomoneda nativa de la blockchain y bloquearlos en una cartera. En función de los fondos que haya en la cartera, mayor será la probabilidad de ser elegido para tener el «privilegio» de validar el siguiente bloque. En caso de que intente actuar maliciosamente, el resto de validadores puede comprobarlo y perdería los fondos bloqueados. Es un sistema que penaliza con pérdidas los comportamientos maliciosos.

En un sistema PoW, el minero tiene dos posibilidades:

- ▶ Actuar correctamente, y obtener una recompensa si valida un bloque.
- ▶ Atacar la red continuamente. Si consigue incluir una operación de doble gasto, el beneficio potencial sería mucho mayor. Se podría incluso deducir que tiene un incentivo económico para comportarse maliciosamente, ya que no existe penalización por ello (más que la potencial pérdida de ingresos por no minar).

En este sistema *Proof of Stake* los actores maliciosos pierden dinero cada vez que intentan jugar en contra de la red.

Otra de las ventajas que tiene este sistema es que no es intensivo en equipo informático. Normalmente vale con tener unos fondos bloqueados en una cartera.

En principio sería un método más accesible para el público general, lo que favorecería la descentralización y se evitaría el monopolio natural del PoW.

Tanto el PoW como el PoS basan su resistencia a ataques en el enorme gasto económico que supone alcanzar un 51% de la capacidad de cálculo o de las

monedas totales de la red. En el sistema PoS, si un atacante quisiera ganar el control sobre la red, tendría que comprar tantas monedas que provocaría un incremento del precio considerable. Cuanto más subiera, más le costaría seguir comprando el volumen suficiente. En la práctica se considera que este tipo de ataque sería económicamente imposible.

Actualmente PoW es un sistema ampliamente testeado y seguro, tal y como se comprueba con Bitcoin y Ethereum. Los sistemas PoS presentan características muy ventajosas respecto a ese sistema (no son intensivos en recursos energéticos), pero a día de hoy hay muchísima menos certeza de que sean tan resistentes en entornos reales. No hay tanta experiencia en su uso y eso lleva a los desarrolladores a ser más cautos.

### ***3.3.3. Mecanismo híbrido PoW/PoS***

Existe una criptomoneda llamada Decred que utiliza un sistema bastante interesante para validar bloques. Los mineros resuelven una prueba criptográfica, y proponen ese bloque para que forme parte de la blockchain. A continuación, se eligen aleatoriamente unos representantes del sistema PoS. Estos tienen que coincidir en que el bloque es válido para que sea efectivamente anexado a la cadena.

Es un sistema diseñado de forma inteligente para repartir el poder entre mineros y usuarios de la red. No olvidemos que el minero es parte de la red por interés económico y puede que quiera que la red evolucione hacia algo que maximice su beneficio en lugar de lo que sea mejor para el proyecto a largo plazo. El

representante PoS normalmente debería de tener un incentivo mayor que el minero para que el proyecto salga adelante en el largo plazo, ya que bloquea sus propias criptomonedas durante un tiempo para tener el derecho de participar como validador. El minero siempre puede cambiar a otra criptomoneda inmediatamente, mientras que el validador tarda más tiempo en poder abandonar la red.

Es un sistema que intenta balancear el poder entre los distintos grupos que intervienen en el sistema.

#### ***3.3.4. Prueba de participación delegada (Delegated Proof of Stake o dPoS)***

Inventado por Dan Larimer, creador de otras plataformas blockchain como Bitshares y Steemit, con los siguientes objetivos en mente:

- ▶ Descentralizar la red, de tal forma que no haya transacciones que puedan ser censuradas. Es decir, que uno o varios nodos decidan no procesarlas de forma voluntaria.
- ▶ Que todos los actores implicados se pongan de acuerdo en el orden en el que suceden eventos en la red.

Se logra de la siguiente forma: Los propietarios de la criptomoneda de la blockchain en cuestión pueden votar qué nodos se encargarán de añadir nuevos bloques a la cadena. Este proceso puede ser diferente según el proyecto, la idea general es que va a haber un número finito de validadores en la red, elegidos, y

que pueden ser revocados por la comunidad.

Se hacen rondas aleatorias para elegir uno a uno a esos validadores, y el elegido ha de proponer qué bloque incluir. Si algo sucede, como que un nodo falla, se desconecta, o no consigue propagar su bloque, el resto de nodos seguirá trabajando sobre la cadena más larga.

Estos nodos tienen un incentivo económico muy alto para tener equipos especializados y operar adecuadamente, porque si no serán sustituidos por otros nodos.

Gracias a este hardware especializado y a que el consenso se tiene que alcanzar por unos pocos nodos, este sistema permite el procesado de miles de operaciones y la creación de bloques cada pocos segundos.

### ***3.3.5. Tolerancia delegada ante fallo bizantino (delegated Byzantine Fault tolerance o dBFT)***

Este sistema de consenso es el utilizado por Neo (entre otros). Los actores que participan en este sistema son los nodos de consenso, pudiendo ejercer dos roles, el de Orador y el de Delegado.

Expliquemos en qué consiste el sistema:

Existen unos nodos de consenso que son los encargados de mantener actualizada la blockchain. Estos nodos de consenso son elegidos aleatoriamente para ejercer el rol de Orador o el de Delegado.

Aquel que es elegido para ser el Orador propone a los Delegados un bloque para

incluir en la cadena. Si por lo menos  $2/3$  de los Delegados están de acuerdo, el bloque se incluye y no podrá eliminado de la cadena. Si hay desacuerdo, se elige aleatoriamente a otro nodo para el papel de Orador y se vuelve a proponer un bloque. Es un proceso iterativo.

Neo actualmente está aún en fase de descentralización, y los únicos nodos de consenso existentes en la red son los autorizados por el propio equipo de Neo. Se supone que a futuro cualquiera podría serlo siempre que cumpla con unos requisitos, sin necesidad de que una autoridad central los valide.

Existen más sistemas de consenso, pero a día de hoy estos son los más extendidos y utilizados por los proyectos más grandes del ecosistema. Seguirán apareciendo nuevos algoritmos que cambiarán unas características por otras, o mejorarán algún punto deficiente. Lo importante es que nos quedemos con la idea de que son mecanismos para decidir qué eventos han tenido lugar en la red y que pasen a formar parte de la cadena.

### **3.4. El trilema de las blockchain**

Actualmente las blockchains presentan un trilema: escalabilidad, seguridad y descentralización.

En el estado actual de la tecnología, existe un *trade-off* entre características, podemos potenciar una a costa de las demás. Para nuestro caso, imaginemos un triángulo, en un vértice tenemos la seguridad; en otro, descentralización y, en el último, escalabilidad.

Entendemos escalabilidad como la capacidad para procesar operaciones que tiene una blockchain. Seguridad como la capacidad para aguantar ataques maliciosos, censura, o el cierre total de la red. Y descentralización como lo distribuido que está el poder entre los actores de la red.

En el estado de desarrollo actual vemos que la mayoría de blockchains solo son capaces de dar solución a dos de estas tres características.



Bitcoin y Ethereum apuestan ambas por la descentralización y seguridad. Cuanto más descentralizado está un sistema, más resistente es a los ataques. Pero como cada operación la tienen que procesar todos los nodos, se pueden realizar menos transacciones por segundo.

Un sistema como EOS recurre a una serie de nodos electos para validar las operaciones. Como es un número de nodos finito (21 más casi 100 de reserva) pueden validar un número muchísimo mayor de operaciones por segundo, es decir, es más escalable, pero a costa de ceder en seguridad y descentralización. Menos nodos hace más sencillo un ataque a la red. Además, el equipo necesario será más especializado, por tanto, más caro y dejará fuera a muchos posibles competidores.

### ■ ¿Entonces, cómo hace un proyecto para decidir qué cualidades elegir?

Eso dependerá de qué intente solucionar dentro del mundo del blockchain. Se trata de elegir qué características tienen más importancia según el problema que se quiera resolver, y tendrán que sacrificar unas cualidades para potenciar otras. Si queremos un proyecto incensurable, no podremos tener solo servidores en un país dependiendo de una sola entidad. Al igual que si queremos tener la capacidad de procesamiento de operaciones que tienen Visa o Mastercard, no podemos pretender alcanzarlo utilizando el protocolo de Ethereum (por lo menos a día de hoy) que, debido a su descentralización y seguridad, tiene problemas de escalabilidad.

## 3.5. Redes blockchain públicas y privadas

Bitcoin es un ejemplo de blockchain pública. Cualquier persona puede participar en ella sin tener que solicitar permiso a nadie. Puede abrir una wallet, hacer transacciones, o incluso participar en el sistema de consenso mediante el minado (en el caso de una cadena PoW) si lo deseas.

Como ya hemos comentado, existen cientos de blockchains, cada una buscando satisfacer necesidades distintas.

Es por ello que existen las blockchains privadas o permissionadas. Estas redes pertenecen a una organización o a una persona, y para poder participar se requiere de una autorización o permiso por parte del propietario.

### ***3.5.1. ¿Qué características tiene una blockchain privada?***

#### **■ Centralizada**

Por definición, si es privada tiene un propietario (o propietarios). El grado de centralización depende de cómo se estructure la red, pudiendo ser relativamente horizontal para la mayoría de participantes. En cualquier caso, no olvidemos que siempre habrá un propietario con más poder sobre los demás, con el riesgo que esto conlleva.

Las ventajas de una descentralización 100% es que no es necesario confiar en ningún participante para tener certeza de que todas las transacciones son seguras. En una red privada, el propietario puede ser un actor malicioso y que no se descubra hasta que ya sea demasiado tarde.

En cualquier caso, los costes de una red permissionada son mucho menores, y no se requiere incentivar a los participantes, por lo que no requiere funcionar con una criptomoneda ni equipos especializados para minar los bloques.

#### **■ Escalabilidad**

En estos sistemas la escalabilidad y el rendimiento son altísimos en comparación con una blockchain pública. Los recursos informáticos destinados a la verificación de las transacciones son triviales respecto a una red proof of work. Esto permite que un solo servidor procese más información a un coste muy bajo.

Además, en una red pública todos los nodos tienen que comprobar la validez de la operación, mientras que en una privada solo lo harán los nodos especialmente designados para ello.

Las redes privadas requieren de una infraestructura concreta, definida por el propietario, donde solo podrán participar los equipos autorizados.

## ■ Privacidad

Estas redes son invisibles para cualquier persona externa, y los participantes de la red solo podrán ver las transacciones para las que hayan sido autorizados.

## ■ ¿Y es necesaria realmente la existencia de blockchains privadas?

Esta es una buena pregunta que frecuentemente hay que contestar. La característica principal de blockchain es que permite las transacciones entre pares sin necesidad de un organismo de confianza. Es resistente a los actores maliciosos. Recordemos que se mantiene una copia de cada operación en los cientos o miles de nodos participantes en la red. Como base de datos es extremadamente ineficiente, y la única razón para pagar esta ineficiencia es obtener a cambio algo más valioso como la resistencia a la censura y a los actores deshonestos.

En una blockchain privada se requiere que confíes en el propietario de la red. La principal característica que hace que elijas una blockchain frente a una base de datos tradicional es eliminada de esta ecuación. ¿Siguen teniendo sentido entonces?

Antes de responder a esa pregunta, vamos a entenderlas mejor. Este tipo de blockchains funcionan de la siguiente manera. Un propietario designa los roles dentro de la red. Cada rol tiene una serie de permisos, siendo lo habitual que uno (o varios) nodos sean los que agreguen operaciones y generen los bloques.

Se podría lograr la misma seguridad con una base de datos bien diseñada, en un entorno en el que intervengan distintos participantes. Pero siempre hay alguien que podría alterar los registros: el propietario.

Con una blockchain permisionada, el propietario no podría hacerlo sin dejar rastro. Esta es lo que hace las blockchains privadas valiosas. Por ejemplo, un conjunto de empresas podría estar operando en una blockchain privada sin aparentes ventajas sobre una base de datos tradicional. Pero actores externos, como el Estado, o los auditores, podrían revisar la información de la cadena y asegurarse de que ni siquiera el propietario de la red ha manipulado los registros.

### **3.6. Hyperledger**

Hyperledger es un conjunto de proyectos open source o de código abierto basados en la tecnología blockchain y organizados por la Fundación Linux. La Fundación Linux es una organización sin ánimo de lucro que promueve proyectos de código abierto y su adopción comercial, tanto para Linux como para otros sistemas operativos.

Muchas de las grandes compañías de software y telecomunicaciones son miembros de la fundación. Ejemplos como Google, IBM, Microsoft, Samsung,

Oracle o Accenture son solo algunos de los nombres de las empresas que colaboran con la Fundación Linux. Con estas grandes empresas no es de extrañar que Hyperledger se haya convertido en el referente por excelencia del blockchain para negocios.

El objetivo de Hyperledger es crear soluciones blockchain, de código libre que utilicen *ledgers* (o libros de contabilidad distribuidos) que ayuden a diferentes industrias a aumentar la eficiencia y a resolver problemas de negocio relacionados con elementos tales como la privacidad de datos, seguridad o compartir información.

Los proyectos de Hyperledger se caracterizan por intentar ser *multi-stakeholder*, esto es un tipo de estructura en el que se intenta que todas las partes participen en el diálogo, la toma de decisiones y la implementación de soluciones. También se busca que los proyectos salgan a producción tan pronto como sea posible, de manera que las empresas puedan usarlo mientras se siguen investigando caminos de mejora y optimización.

Las cadenas de bloque son privadas, lo que significa que los participantes que se unen a la red son autenticados a través de un módulo de identificación. Esto sirve para reducir el riesgo de que actores maliciosos se metan dentro de la red.

Además, dentro de Hyperledger, las transacciones solo son visibles para las partes envueltas en la transacción. Así nos aseguramos de que, si tenemos acuerdos privados, estos no puedan ser visualizados por terceros.

Como bien sabemos, en las blockchain públicas cualquiera puede unirse a la misma, así como crear nuevas transacciones o leer el histórico de las mismas. Si queremos una blockchain aplicada a un negocio privado, estos elementos pueden

ser no deseables.

En resumen, Hyperledger ofrece las capacidades de una estructura blockchain: la privacidad de datos, compartir información entre los diferentes actores y la inmutabilidad de los registros, todo ello con un conjunto de protocolos de seguridad enfocado a la empresa.

### ***3.6.1. Proyectos de Hyperledger***

Hyperledger consta de diez proyectos, dentro de los cuales cinco son *frameworks* de libros de contabilidad distribuidos: Fabric, Iroha, Sawtooth, Burrow e Indy. Los otros cinco son módulos que apoyan estos frameworks y son: Composer, Explorer, Quilt, Cello y Caliper.

#### ***3.6.1.1. Frameworks de Hyperledger***

Antes de ver cuáles son los diferentes frameworks que tiene Hyperledger vamos a definir qué es un framework. Un framework es un entorno de trabajo con una estructura definida y con unas reglas y condiciones que hay que cumplir.

- **Fabric:** Fue el framework pionero de Hyperledger. Con una arquitectura modular, este framework hace posible la creación de canales a través de los cuales se produzcan transacciones confidenciales sin tener que pasar la información a una autoridad central. Este framework recoge el trabajo de Digital Asset Holdings, Blockstream e IBM. Es el proyecto que más rápido

ha crecido dentro de Hyperledger.

- ▶ **Iroha:** Se trata de una construcción simple y moderna implementada en el lenguaje de programación C++ que usa un algoritmo de consenso llamado YAC (Yet Another Consensus). Inspirada por Fabric, se intenta complementar focalizándose en el desarrollo de aplicaciones móviles para Android e iOS.
- ▶ **Sawtooth:** Utiliza una plataforma modular para construir, desplegar y ejecutar libros de contabilidad distribuidos. El diseño de Sawtooth permite a las aplicaciones elegir sus reglas de transacciones, los permisos y los algoritmos de consenso que ayuden a la necesidad de su negocio, cambiando los mismos en el momento conveniente. Tiene una versatilidad al soportar tanto despliegues de blockchain permissionadas como no permissionadas. Además, todos los nodos disponen de la misma información.
- ▶ **Indy:** Permite a los usuarios verificar la identidad de alguien basándose en la información que esa misma gente está dispuesta a mantener y compartir. La privacidad de datos resulta cada vez más crucial para las empresas. Hyperledger Indy apuesta por descentralizar esta información de manera que sea cada persona la dueña de su propia información y que ella misma de permisos de qué información quiere compartirse, siendo además interoperable entre dominios administrativos o aplicaciones. La responsabilidad de las empresas disminuiría al no ser ellos quien manejara la información de sus clientes.
- ▶ **Burrow:** Inicialmente desarrollada por Monax, provee un cliente modular de blockchain con una máquina de *Smart contracts* (o contratos inteligentes, explicaremos más adelante en qué consisten) y un intérprete incorporado en la

especificación de la Máquina Virtual de Ethereum o *Ethereum Virtual Machine* (EVM).

#### **3.6.1.2. Módulos de Hyperledger**

A su vez, los módulos de Hyperledger son software que apoyan a los frameworks vistos a través de distintas funcionalidades.

- **Composer:** Construido sobre Fabric, este módulo facilita una serie de herramientas que permiten crear redes de blockchain para negocios.

Es una herramienta muy potente, ya que permite crear un MVP (*Minimum Viable Product* o Producto Mínimo Viable) o prototipos de manera rápida que permitan evaluar la viabilidad de un producto. En un mundo donde la filosofía *Agile* está cada vez más implementada en las empresas, Composer nos ayuda a no gastar recursos de tiempo y dinero antes de comprobar la verdadera funcionalidad del proyecto.

La herramienta se puede implementar de manera local, pero también tenemos una herramienta online llamada *Composer playground* donde podemos crear nuestra primera blockchain, definir a los participantes, los productos y realizar las primeras transacciones.

Otro de los grandes atractivos de Composer es que permite generar una interfaz que permite interaccionar con la blockchain de forma sencilla sin requerir conocimientos de programación.

Finalmente, con Hyperledger Composer podemos crear REST API contra las

que crear aplicaciones rápidamente. Aunque tengamos una red blockchain privada, necesitamos una aplicación web para que los diferentes actores puedan interactuar con la blockchain, ya sea introduciendo nuevas transacciones o activos o leyendo las transacciones pasadas. La REST API nos permite poder llamar a las funciones necesarias para crear y consultar transacciones.

- ▶ **Explorer:** Esta herramienta permite interaccionar con una blockchain. Dispone de una interfaz web que permite monitorizar e interactuar con la red de manera visual. Al igual que Composer, trabaja sobre Fabric y también proporciona una REST API.
- ▶ **Quilt:** Esta herramienta ofrece interoperabilidad entre sistemas de ledgers o libros de cuentas mediante Interledger o ILP, un protocolo de pagos destinado a transferir valor entre ledgers distribuidos y no distribuidos. Es una herramienta con mucho potencial, ya que permitiría a cadenas de distintos tipos de Hyperledger conectarse entre ellas.
- ▶ **Cello:** Se trata de un módulo cuyo objetivo es ofrecer blockchain como un servicio, reduciendo así el esfuerzo requerido para montar, administrar y terminar blockchains. Con Hyperledger Cello se puede mantener un pool de blockchains en la nube a través de elementos como máquinas virtuales y monitorizar el estado de las mismas.
- ▶ **Caliper:** Esta herramienta permite a los usuarios medir el rendimiento de la implementación de una blockchain mediante casos de uso predefinidos. Hyperledger Caliper genera informes con indicadores como TPS (Transacciones Por Segundo) o latencia de transacción entre otros, de manera

que los resultados puedan ser utilizados por otros proyectos referencia para la elección de la implementación de una blockchain que se adecúe a las necesidades específicas de cada uno.

Ahora que hemos visto los diferentes proyectos dentro de Hyperledger, vamos a estudiar un escenario particular donde podemos aplicar el proyecto principal de Hyperledger, el framework Fabric:

Cada año en España se conocen noticias de delitos relativos a la propiedad industrial por comercializar vino usando ilegítimamente etiquetas con denominaciones de origen. Esto supone pérdidas de cientos de miles de euros para las bodegas y un desprestigio injusto para aquellas que producen productos de calidad, ya que un consumidor que no sepa que el producto es falsificado pensará que la calidad recibida es culpa de la bodega. Se trata, por lo tanto, de una industria que podría beneficiarse de la innovación y de la transparencia que puede aportar el blockchain.

¿Y cómo puede solucionar Hyperledger Fabric este y otros problemas? Para explicarlo, vamos a describir las diferentes partes que intervienen en el proceso:

- ▶ Alicia lleva una bodega donde produce vino con denominación de origen.
- ▶ Bruno es el propietario de un restaurante en Italia que sirve el vino de Alicia.
- ▶ Cristina es también propietaria de otro restaurante en China.
- ▶ Daniel gestiona una empresa de transporte con la que opera Alicia.
- ▶ Los reguladores verifican las condiciones sanitarias del vino.

Los elementos de Hyperledger Fabric son los siguientes:

- ▶ Los canales: La parte más potente de Fabric son mecanismos que permiten que solo los miembros del canal puedan ver las transacciones que se producen en el mismo. Cada canal es una cadena independiente de bloques que contiene únicamente las transacciones que se han producido en ese canal.
- ▶ Los Smart contracts (también se conocen como *chaincode*): Contienen tanto la definición de los activos como la lógica de las transacciones que modifica características de los mismos.
- ▶ El estado del mundo o *world state*: Refleja los datos actuales de todos los activos en la red.
- ▶ El ledger: Contiene el world state de la red, así como una cadena de las transacciones efectuadas.
- ▶ La red: Es el conjunto de los miembros (*peers*) que forman la red. Esta red es responsable de mantener una copia consistente del ledger.
- ▶ El servicio de ordenación: Es un conjunto de nodos que ordenan transacciones en un bloque.
- ▶ El servicio de provisión de membresía o *membership service provider* (MSP): Administra las identidades y el acceso a clientes y miembros.

Para explicar el proceso, empecemos con la bodega de Alicia, quien trabaja como negocio familiar con ventas internacionales. Mediante una aplicación, Alicia es capaz de acceder a la blockchain donde se encuentran otras bodegas como la suya, además de propietarios de restaurantes y reguladores. Alicia puede añadir o actualizar información a medida que el vino avanza en la cadena de suministro. A este ledger tienen acceso tanto los restaurantes, la empresa de

transporte y los reguladores.

Cada vez que se produce una botella de vino, Alicia registra la información de manera automática asignando un identificador, la localización, el tiempo de embotellamiento, etc. Estos detalles se guardan en el world state basándose en las especificaciones del Smart contract, permitiendo a la aplicación de Alicia crear una transacción en el ledger.

Imaginemos que Alicia vende a 5 € la botella de vino al restaurante de Cristina, mientras que con Bruno tiene un acuerdo en el que vende cada botella a 3. Alicia no puede aceptar una blockchain pública, ya que Cristina podría mirar el precio al que Alicia está vendiendo las botellas a Bruno y exigir una reducción. Sin embargo, Alicia sí quiere que el resto de participantes vean los detalles de cada botella. Con Hyperledger Fabric esto es posible, ya que Alicia mantendría un canal con cada uno de los restaurantes en el que solo ellos podrían ver los precios acordados.

El transportista también tendría acceso a la blockchain para confirmar y ver los detalles del ledger. Podría confirmar la orden del transporte, así como especificaciones sobre posibles penalizaciones en caso de entregar con retraso un pedido, aplicándose esta reducción de manera inmediata gracias a los Smart contracts. De esta manera, se optimiza el proceso y elimina las posibles discusiones sobre la entrega. También aumentaría la confianza en el transportista si podemos ver su histórico de los tiempos de entrega.

Finalmente, el regulador tendría acceso de lectura al ledger para confirmar y estudiar los detalles del mismo y tomar acciones inmediatas en caso de detectar alguna irregularidad.

Hemos visto que se mantiene una trazabilidad completa de cada producto a lo largo de la cadena de suministro. Esto trae muchos beneficios como, por ejemplo, poder detectar el origen y el día de una botella que se encuentre en mal estado. Además, el consumidor final aumenta su confianza porque puede comprobar de manera segura que está comprando un producto con unas características concretas.

Como se puede ver, este ejemplo es replicable para muchos productos con denominación de origen y, en general, en la cadena de suministro de cualquier industria. De la misma manera, otras industrias pueden verse favorecidas gracias a Hyperledger y está en la mano de cada empresa estudiar cuál de los frameworks se adecúa más a sus necesidades.

Existen otros productos que usan ledgers distribuidos como Chain Core, Corda o Quorum. Estas iniciativas tienen estados de desarrollo muy diferente, y realmente donde a día de hoy vemos que se concentra el potencial desarrollador es en Hyperledger.

### **3.7. Casos de uso del Blockchain**

Los casos en los que podemos aplicar la tecnología de blockchain son muy variados. A continuación, vamos a poner diferentes ejemplos para entender el alcance que puede tener y la revolución que supone:

- ▶ Acuerdos entre particulares
- ▶ Aseguradoras

- ▶ Derechos de autor
- ▶ Identidad portable
- ▶ Internet of Things
- ▶ ONG
- ▶ Sector Backoffice
- ▶ Sector bancario
- ▶ Sector transporte
- ▶ Transparencia
- ▶ Votaciones

## ■ Acuerdos entre particulares

Se podrían realizar acuerdos entre particulares y que se ejecutaran de forma autónoma mediante Smart contracts (o contratos inteligentes).

Un ejemplo podría ser un préstamo entre dos familiares. El familiar A le deja 10.000 € al familiar B y mediante un Smart contract el familiar B le va devolviendo el dinero al A en las fechas correspondientes y con el interés pactado previamente.

Gracias a hacerlo de esta forma conseguimos aumentar la transparencia en todo el proceso y, además, que se ejecuten pagos de dinero al cumplirse las condiciones que se pactaron.

Si nos ponemos a pensar en casos de usos domésticos podremos encontrar una gran cantidad de ejemplos que nos facilitarían algunas de las relaciones entre

particulares.

Una aplicación muy concreta y curiosa se conoce como *dead man switch*. Básicamente consiste en que, si una persona muere, se ejecuta un Smart contract automáticamente. Podría ser para pasar información muy sensible a herederos.

## ■ Aseguradoras

En el sector de los seguros, la tecnología blockchain y los contratos inteligentes o Smart contracts pueden tener una implicación muy positiva tanto para el usuario final como para la aseguradora.

Gracias a la tecnología de los contratos inteligentes se podrían gestionar de forma automática los cobros de las indemnizaciones.

Podríamos comprar un seguro de vuelo por si el avión se retrasara en la llegada al país de destino y mediante los contratos inteligentes podríamos cobrar el seguro en el momento que ocurriera un retraso.

Con esto conseguiríamos no tener que hacer reclamaciones a la compañía aseguradora y olvidarnos de los diferentes temas burocráticos que existen en la actualidad para poder hacer el cobro del seguro.

Podríamos comprar este seguro minutos antes del vuelo, y cobrarlo inmediatamente si se produce el evento contra el que nos hemos asegurado.

## ■ Derechos de autor

Se puede grabar en blockchain la propiedad de un artista, cantante, pintor, etc., y

demostrar la fecha con la que se hizo el registro en la blockchain para autenticar la autoría de la obra.

Gracias a poder registrar cualquier cosa en la cadena de bloques luego sería muy fácil ver quién fue el que registró una canción y así poder prescindir de la figura de un notario que certifique la autoría. Con esto también se conseguirían bajar los costes para demostrar los derechos de autor.

Además, también se podría hacer que mediante los Smart contracts se pagara a los autores de las obras cuando sean descargadas. Al descargarse el disco de un grupo de música se podría hacer que directamente se les enviara el dinero a su wallet.

## ■ **Identidad soberana**

Se podría crear una blockchain donde cada usuario tenga un identificador único y el acceso a su identidad en la red. Este usuario podría autorizar a otros usuarios a ver su perfil durante el tiempo que él considere oportuno y solo a los datos que quiera mostrar.

Es un caso de especial importancia a día de hoy, en el que vemos que refugiados de guerra que no tienen ningún documento que demuestre su identidad tienen serios problemas para ser acogidos por otros países. Un registro online e inmutable podría solucionarlo con relativa facilidad.

Otro problema que podría resolver son las continuas brechas de seguridad de las empresas que acaban perdiendo datos personales de miles de usuarios. Esta información puede ser muy sensible y comprometer la seguridad de los

afectados. Si nosotros somos los únicos dueños de nuestra información, y podemos compartirla y revocar el acceso fácilmente, se podrían evitar estos sucesos.

## ■ Internet of Things (IoT)

*Internet of Things* o «internet de las cosas» es como se conoce al concepto de interconectar de forma digital a diferentes objetos con una red, que normalmente es internet.

*Internet of Things* unido a la cadena de bloques nos ayuda a grabar en ella las lecturas de diferentes sensores y, dependiendo de esas lecturas, ejecutar de forma autónoma otros procesos mediante los Smart contracts.

La parte de IoT puede estar muy relacionada y ser muy útil dentro de las empresas para el control de calidad. Podríamos tener un sistema totalmente automatizado, que grabe información directamente en la blockchain sin intervención humana, y tener certeza de que no ha sido manipulada.

## ■ ONG

La ventaja que obtenemos al aplicar la tecnología de cadena de bloques a las ONG es la transparencia que se gana en todo el proceso de recaudación y uso de los fondos. Sería posible hacer la trazabilidad del dinero que se ha donado a ONG y ver el uso real que se está dando del mismo.

Esto sería útil para generar más confianza en estas entidades, ya que siempre puede haber personas reticentes a donar debido a que desconoce cuál es el

destino de las aportaciones que hace.

## ■ Sector Backoffice

Para el sector Backoffice, gracias a la tecnología de cadena de bloques podemos ahorrar en costes de contabilidad, auditoría y regulación.

Es posible estar conectado en tiempo real a toda la información de la contabilidad y que se realicen informes automáticos mediante contratos inteligentes. Además, tanto para el regulador como para una auditoría de las cuentas se podría consultar la información y comprobar que es veraz, ya que la trazabilidad es absoluta. Y olvidarnos de tediosos procesos de contrastar fuentes de información para dar veracidad a un hecho.

## ■ Sector bancario

Dentro del sector bancario encontramos multitud de ventajas que nos ofrece blockchain.

El primer ejemplo sería el de transferencias más rápidas y baratas. Gracias a las criptomonedas es posible hacer transferencias a nivel mundial casi instantáneas y con comisiones prácticamente despreciables.

El segundo ejemplo sería el de ahorro en auditoría. Al utilizar blockchain para registrar las diferentes operaciones del banco se consigue poder hacer una trazabilidad a toda la información y poder automatizar informes de control. De esta forma se consigue un ahorro en auditorías, tanto internas como las que llevan a cabo las Administraciones Públicas.

## ■ Sector transporte

Se podría gestionar toda la trazabilidad de cualquier artículo registrando en cada punto de control la información en la cadena de bloques, así se podría saber en qué momento de la cadena se encuentra y si ha sufrido algún tipo de percance.

En muchas de las empresas actuales que tienen un gran stock es común tener partidas de objetos que no se sabe en qué parte del almacén se encuentran por no haber hecho bien el control de stock. Si todo se gestionara mediante blockchain quedaría un registro perfectamente trazable y se podrían encontrar los objetos de forma inmediata. Aparte de la trazabilidad se podría también añadir contratos inteligentes para controlar en todo momento los estados tanto de los camiones como de las fábricas (temperatura, velocidad, vibración, etc.) y poder lanzar avisos de forma automática a los controles de calidad en caso de que alguno de los parámetros tuviera un valor anormal.

Además, gracias al registro en blockchain también se podría combatir toda la falsificación porque se podría ver la procedencia de los productos y el número de unidades que salieron desde la fábrica. De esta forma nos aseguramos de que en ningún momento de la cadena se añadan nuevos productos al envío y podemos comprobar el punto de partida de los objetos.

En productos perecederos podríamos saber en todo momento la fecha de recogida/elaboración, el origen, productos utilizados para el crecimiento de las frutas/hortalizas, temperatura en el transporte, temperatura en los almacenes, etcétera.

## ■ Votaciones

A la hora de hacer votaciones es muy común que existan discrepancias sobre cómo se ha realizado el recuento de votos y si ha sido alterado en algún momento.

Si quedaran todos los votos registrados en blockchain se podría hacer el recuento de forma automática y además conseguir una transparencia absoluta. Para ello sería necesario que cada persona que pudiera votar tuviera asignado algún identificador único (para poder identificarlo de forma unívoca) y que los votos quedaran registrados dentro de la cadena de bloques. Se podría saber que la persona ha votado, sin que se sepa a quién ha votado.

También se podría hacer que una vez finalizara el periodo de votaciones se leyeran todos los votos de la cadena de bloques y se ejecutaran diferentes acciones de forma automática gracias a los contratos inteligentes.

## Conclusión

Hemos visto cómo la tecnología blockchain permite muchas cosas más allá del Bitcoin. Y que no todas las blockchains son iguales. Las hay más rápidas y más lentas, algunas tienen mineros y otras no, pueden apostar por una cierta centralización o incluso ser privadas. Hay una infinidad de posibilidades, y cada configuración tendrá sentido para un caso de uso concreto.

No hay una blockchain definitiva que sirva para todo. Pero lo que hemos aprendido es que permiten cierto grado de personalización para satisfacer unas

necesidades concretas. Dependerá de los desarrolladores elegir la mejor configuración para las condiciones bajo la que esta tenga que ser operada.

## 4. Ethereum y más

### 4.1. Ethereum

Ethereum, al igual que Bitcoin, está basado en blockchain. Pero con una diferencia fundamental, Ethereum utiliza un lenguaje de programación Turing completo<sup>[35]</sup>. Esto, de forma muy simplificada, significa que utiliza un lenguaje que se puede aplicar a diferentes problemas computacionales y con el cual se consiguen implementar diferentes estructuras complejas tipo bucles. Mientras que Bitcoin tiene la función de ser una herramienta para intercambio de valor entre usuarios, Ethereum nace para ser una plataforma donde ejecutar programas de forma descentralizada.

Ethereum recibe el nombre de «ordenador mundial» porque consiste en miles de nodos comunicándose continuamente entre sí, para ponerse de acuerdo en qué es lo que está sucediendo en la red.

Al haber tantos ordenadores procesando la misma información a la vez, es resistente a la censura. Nadie tiene poder para impedir que se dejen de procesar las transacciones, pero tiene una contra, la información tiene que ser procesada por todos los nodos, lo que hace que sea un sistema muy lento y difícilmente escalable.

En Ethereum los programas son escritos a través de Smart contracts o contratos inteligentes. Estos contratos son piezas de código autoejecutable que se alojan permanentemente en la blockchain, y que siempre que son invocados realizan la secuencia para la que han sido diseñados.

Dentro de esta plataforma existe una unidad monetaria llamada ether. Su función principal es servir como medio de pago por la capacidad computacional que se usa, aunque, además, al igual que bitcoin también se utiliza para hacer transferencias económicas.

Definiendo Ethereum en una sola frase quedaría de la siguiente forma: *Ethereum es una plataforma basada en tecnología blockchain que permite desplegar programas autoejecutables y resistentes a la censura. Es una red que no pertenece a nadie y que se rige por mecanismos de consenso.*

Respecto a la parte de pagar por la capacidad computacional, vamos a desarrollarlo un poco más. Cuando realizamos una transferencia o ejecutamos un Smart contract, todos los nodos de la red tienen que procesar los cambios de estado que se producen. Es decir, dedican recursos para realizar los cálculos necesarios.

Para pagar por el uso de estos recursos, existe un concepto llamado *gas*. Cuando realizas transferencias, ejecutas un contrato, o interactúas con la blockchain de alguna forma, tienes que pagar por el uso de recursos. Este coste se mide utilizando la unidad gas, y el pago se hace en ethers. El coste se calcula de la siguiente forma:

$$\text{Coste de transacción} = \text{Precio de gas} \times \text{Límite de gas}$$

El precio del gas lo puede modificar el usuario y sirve para indicar cuánto está dispuesto a pagar por unidad de gas. Cuanto mayor sea, más posibilidad de que los mineros acepten la transacción casi inmediatamente. Realmente estás pujando por garantizar que tu operación tiene hueco en el siguiente bloque. La

unidad de medida es el GigaWei (GWei), siendo la unidad más pequeña de un ether el Wei:

$$10^9 \text{ Wei} = 1 \text{ GWei}$$

$$10^{18} \text{ Wei} = 1 \text{ Ether}$$

Wei es la mínima unidad divisible de un ether, al igual que un satoshi es la mínima unidad divisible de un bitcoin.

El límite de gas es el número máximo de gas que el usuario está dispuesto a pagar teniendo en cuenta lo siguiente:

Diferentes interacciones tienen diferentes costes<sup>[36]</sup>. A una transacción normal se le suele poner un límite de 21.000 gas, mientras que operaciones más complejas tendrán que tener un límite superior. Si enviamos una transacción con un límite de gas de 15.000, los mineros la verán, empezarán a ejecutarla, y cuando se acabe el gas la dejarán abandonada y fallará. Pero como ya han dedicado recursos a procesarla, el usuario pierde la comisión. Normalmente recibiremos instrucciones de qué límite debemos poner tanto por el programa que usemos como por los creadores de Smart contracts.

El límite de gas existe para que no ejecutemos una operación y se quede iterando hasta el infinito por algún fallo.

¿Y por qué Ethereum usa este sistema de costes?

Esto se hace por distintas razones.

1. Se evita malgastar recursos. Al tener un coste de ejecución, se penaliza el código escrito de forma poco eficiente.

2. Impide que un programa repita una operación hasta el infinito. De esta forma, ante un fallo en el código, podemos prevenir, por ejemplo, que se sigan enviando fondos desde nuestra cuenta a otra hasta dejarla vacía.
3. Previene los ataques tipo spam. Si la ejecución de Smart contracts y transacciones no tuviera un coste, un actor malicioso podría decidir lanzar miles de programas a la vez para saturar la red y conseguir que esta sea incapaz de procesar las operaciones legítimas. Al tener un pequeño coste, se consigue que este tipo de ataques sean extremadamente caros de ejecutar.

Al igual que en Bitcoin, actualmente el algoritmo de consenso se basa en prueba de trabajo (PoW). Se prevé que en un futuro migre hacia un sistema prueba de participación (PoS), ya que en la práctica se está comprobando que con algoritmos PoW se tiende a la centralización y, además, el coste en recursos aumenta.

En Ethereum, los bloques se generan cada 15 segundos aproximadamente, y el tamaño del bloque viene determinado por un límite de gas de 8 millones. Los mineros tienen la libertad de decidir imponer un límite de tamaño menor o mayor, teniendo en cuenta que si lo aumentan la velocidad de propagación puede verse afectada. Cada bloque resuelto tiene de recompensa una parte fija de 3 ethers, más una parte variable. En lo que va de 2018 la recompensa promedio por bloque minado es de unos 3,56 ethers.

Para minar Ethereum la mayoría de personas utilizan GPU (tarjetas gráficas de PC) y aunque en teoría esto permite una mayor descentralización, ya que cualquiera puede montar el equipo en casa, la realidad es que prácticamente el 100% del mercado de las GPU está en manos de dos competidores, AMD y

NVIDIA. Si alguno de estos dos fabricantes decidiera integrar en ellas un software con algún fin maléfico las repercusiones podrían ser devastadoras.

Recientemente, el principal fabricante de equipos ASIC para Bitcoin ha sacado un minero especializado para Ethereum. La penetración de estos equipos se suele notar en los mercados por un aumento del hashrate en los meses previos al lanzamiento del equipo. En cualquier caso, está por ver si la comunidad de Ethereum decide cambiar el algoritmo para dejar obsoletos estos equipos.

Ethereum nace con el propósito de ser una plataforma descentralizada para la ejecución de *dApps (decentralized applications)*. Una dApp es una interfaz para que el usuario pueda interactuar de forma sencilla con la blockchain, a través de Smart contracts programados por desarrolladores.

La verdadera revolución que ha supuesto Ethereum es la facilidad con la cual se pueden crear tokens, y gracias a ello, se han generalizado las ICO (Initial Coin Offering). Más adelante hablaremos largo y tendido sobre ellas, de momento, nos vale con entenderlas como un mecanismo de financiación para proyectos basados en blockchain mediante *crowdfunding*.

El crowdfunding es una forma de financiar proyectos de forma colaborativa, es decir, un proyecto se financia con microaportaciones de diferentes personas.

A finales de agosto de 2018, la web de CoinMarketCap tenía 1.910 criptoactivos listados, de los cuales 1.048 eran tokens y, de esos tokens, 917 estaban basados en Ethereum, por lo que tenía una predominancia entre las plataformas de Smart contracts de aproximadamente el 88% del total.

Un token consiste en un criptoactivo, cuya finalidad es la de interactuar con una plataforma (*token utility* o de utilidad) o tener derecho a un rendimiento

económico (*token security*).

Gracias a la novedosa forma de captar financiación de las ICO, cientos de proyectos han lanzado su propia moneda utilizando Ethereum como plataforma con el fin de recaudar dinero para construir un proyecto.

Haciendo referencia al artículo de *Fat Protocols*<sup>[37]</sup> de Joel Monegro, si la plataforma subyacente es utilizada para construir proyectos, esto le hace crecer en valor. Por ello vemos potencial en que Ethereum siga evolucionando, ya que la gran mayoría de proyectos del ecosistema han sido lanzados sobre ella. Al concentrar un volumen tan alto de desarrolladores, puede avanzar más rápido y captar más inversión que otras blockchains.

Más adelante hablaremos del capital recaudado a través de las ICO, y la importancia que ha tenido para atraer inversión al sector y a desarrolladores.

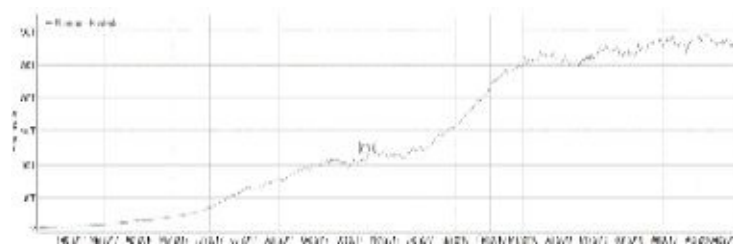
En la siguiente imagen, podemos ver que desde enero de 2017 las transacciones en la red han aumentado y finalmente se han ido manteniendo en unas 600.000 transacciones diarias.



Fuente: <https://bitinfocharts.com/comparison/ethereum-transactions.html>

Además, también podemos comprobar en la siguiente imagen como el hashrate ha crecido de forma notoria hasta mantenerse más o menos constante a partir de

marzo del 2018. Recordemos que el hashrate es la capacidad computacional minando en la red. Cuanto más crece, significa que más gente está apostando por el futuro de esta blockchain y están realizando inversiones en nuevos equipos.



*Fuente: <https://bitinfocharts.com/comparison/ethereum-hashrate.html>*

Por último, la red de Ethereum se ha visto colapsada en varias ocasiones, por ejemplo, en el momento del lanzamiento de una ICO, o cuando mucha gente ha interactuado a la vez con un juego de gatitos coleccionables llamado CryptoKitties, que causó furor en diciembre.

El colapso se traduce en que las operaciones tardan horas en ejecutarse, o hay que pagar comisiones muy altas para que tengan prioridad y sean minadas.

Se están trabajando en varias soluciones que aportarían escalabilidad a la red. Entre ellas estarían las soluciones off-chain, es decir, transacciones que tienen lugar fuera de la cadena principal. Es una solución similar a Lightning Network en Bitcoin. Y otra de las soluciones en las que se está trabajando, llamada Plasma, consiste en la creación de distintas *child-chains* (cadenas hijas que dependen de la principal) de manera que cada child-chain tiene un protocolo de consenso independiente de la cadena principal, y los criptoactivos se pueden transferir entre ellas cuando sea necesario.

Ambas aliviarían a la cadena principal de tener que procesar todas y cada una de las transacciones que tengan lugar en la red. Estas soluciones están en fase experimental, pero avanzan a un ritmo muy rápido y no sería raro verlas en funcionamiento a lo largo de 2019.

## **4.2. Clasificación de los activos digitales**

Uno de los problemas de fondo que tenemos en este mundo de los activos digitales es el siguiente:

¿Cómo categorizamos todos los activos existentes?

Si somos muy estrictos, muchos de ellos caerían en diferentes categorías, haciendo imposible clasificarlos o llevando a error. Preferimos en este caso utilizar unas categorías muy amplias que permitan al lector tener un esquema mental rápido para entender a qué criptoactivo se está enfrentando.

### **4.2.1. Criptomonedas o criptodivisas**

La función exclusiva de este activo digital es transferir valor de un usuario a otro. Nos da igual si es para pagos pequeños del día a día, si es para pagar una casa, o si actúa como reserva de valor (*store of value*). Son medios de pago.

Es común ver en esta categoría una subdivisión, las *altcoins*. Las altcoins son «alternative to Bitcoin», es decir, son todas las criptomonedas que no son

Bitcoin.

No le vemos sentido dividir esta categoría en «Bitcoin» y «todas las demás», por lo que para nosotros todas entran en la clasificación de criptomonedas o criptodivisas.

¿En qué se diferencia una criptodivisa de otra?

Como ya hemos visto, estamos hablando de software personalizable, por lo que al final existen cientos de criptomonedas con ligeras variaciones entre sí para cubrir una necesidad.

Tenemos por ejemplo Monero, que no permite conocer las partes implicadas en el envío y recepción de la criptomoneda, ni los balances de las cuentas. Tenemos las *stablecoins* como Tether, cuyo objetivo es guardar una relación 1:1 con una divisa fiat como es el dólar (dinero cuyo respaldo es un gobierno). Otras procesan los bloques casi instantáneamente, o utilizan algoritmos de consenso diferentes.

Resumiendo, existe una extensa variedad dentro de la categoría criptomoneda, y creemos que crear una subdivisión no ayuda a entenderlas mejor, y en cambio sí puede dar lugar a confusión.

#### **4.2.2. Plataformas**

El fin de estos protocolos no es la transferencia de valor como tal, aunque se utilicen así en muchas ocasiones. Estas plataformas permiten mayor funcionalidad gracias a que se pueden escribir programas complejos sobre ellas,

habilitando la construcción de aplicaciones descentralizadas (dApps) mediante Smart contracts. Sirven como base donde desarrollar un ecosistema de proyectos que cumplan distintas funciones.

La más conocida es Ethereum, aunque otras que compiten en este espacio son NEO, EOS, NEM, AION...

Capturan valor en función de los proyectos que se construyan sobre ellas. Actualmente casi todos los proyectos se lanzan sobre Ethereum. Cuantos más proyectos se lanzan sobre ella, más valor tiene la red, y cuanto más valor tiene la red, más incentivo hay para trabajar sobre ella.

Sobre estas plataformas se crean los tokens. Los tokens recordemos que son activos digitales que permiten interactuar con un proyecto en concreto o que permiten tener unos beneficios económicos.

### **4.2.3. Tokens**

Los tokens nacen en un Smart contract desplegado en una plataforma y, como dijimos anteriormente, los más habituales son los que residen sobre Ethereum.

Su función más habitual es la de actuar como medio de pago en su propio ecosistema, es decir, en su dApp y normalmente se usan para pagar por usar los servicios que ofrecen.

Y aunque la función que predomina es la de pagar por unos servicios, también existen otras funciones que dan, por ejemplo, derecho a voto, derecho sobre beneficios, derecho sobre unos activos físicos concretos, etcétera.

¿Y por qué no utilizan directamente ether en lugar de un token?

Hay varias ventajas al emitir un token:

- ▶ Definir cómo se comporta el token en la plataforma.
- ▶ Determinar un suministro máximo, generando una escasez.
- ▶ Mecanismo de financiación (a través de una ICO).

En resumen, según esta clasificación tenemos tres categorías.

- ▶ Criptomonedas, que son medios de pago.
- ▶ Plataformas, que permiten desplegar contratos inteligentes y crear dApps. Sobre ellas residen los tokens.
- ▶ Tokens, que son activos digitales que otorgan ciertos derechos, como usar un servicio o votar.

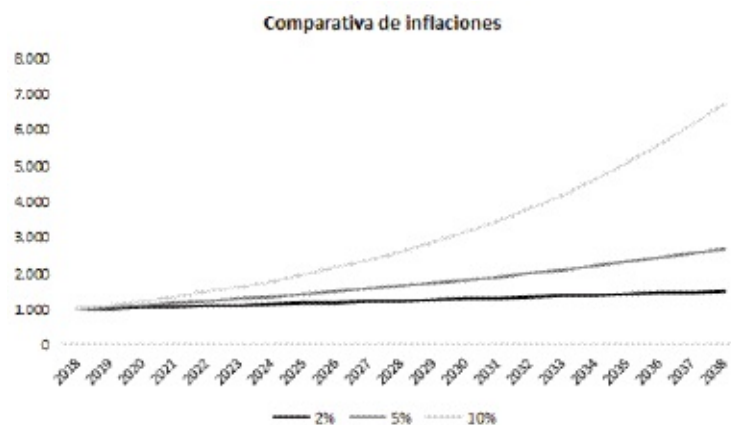
### **4.3. Inflación y deflación**

El concepto de inflación lo oímos continuamente, y tiene mucha relevancia en el mundo de las criptomonedas. Recordemos que al final se trata de crear un sistema económico al margen de las instituciones, y como todo sistema económico se verá afectado por inflación, oferta monetaria, etcétera.

La inflación en el sentido que todos conocemos consiste en el aumento de precios con el paso del tiempo. El objetivo<sup>[38]</sup> del Banco Central Europeo es mantener esta inflación inferior al 2%, aunque próxima a este número. Esto se

traduce en que, según va pasando el tiempo, nuestro dinero puede comprar menos bienes y servicios.

Hemos construido un ejemplo a continuación de cómo afectan diferentes niveles de inflación al poder adquisitivo con el paso de los años. En la gráfica comenzamos 2018 con 1.000 euros en el bolsillo, y vemos la cantidad de dinero que nos haría falta cada año para mantener el mismo poder adquisitivo, en escenarios del 2%, 5% y 10% de inflación.



*Fuente: Elaboración propia*

En el primer escenario, donde teníamos una inflación del 2%, necesitaremos tener aproximadamente 1.486 € veinte años más tarde para poder comprar lo mismo que podíamos comprar en el 2018 con 1.000 €. Para el segundo escenario necesitaremos la cantidad de 2.653 € para tener la misma capacidad de compra que teníamos en el 2018; y, por último, para la inflación del 10% (tercer escenario) necesitaremos la cantidad de 6.727 €.

Como podemos comprobar, cuanto más alta es la inflación más rápido sube el

precio de todos los bienes y servicios, es decir, se encarece la vida. O menos vale nuestro dinero. Si tenemos dinero ahorrado en una cuenta bancaria, estará perdiendo poder adquisitivo de forma continua.

El dinero que tendríamos que tener en 2038 con cada una de las inflaciones para tener la misma capacidad de compra que teníamos en 2018 con 1.000 € son:

- ▶ Inflación al 2%: Deberíamos tener aproximadamente 1.486 €.
- ▶ Inflación al 5%: Deberíamos tener aproximadamente 2.653 €.
- ▶ Inflación al 10%: Deberíamos tener aproximadamente 6.727 €.

Por lo tanto, es fácil darse cuenta de que, si tenemos una inflación alta, la velocidad con la que perdemos poder de compra es muy rápida. Si comparamos la inflación del 10% con la del 2% comprobamos que necesitamos más de cuatro veces del dinero para poder comprar los mismos productos. En el escenario de la inflación al 10%, pasados 20 años las cosas nos costarían casi siete veces más que en 2018.

En economías occidentales suele haber una inflación constante entre el 2-3%. Si los salarios no suben al mismo ritmo que la inflación, provoca una pérdida gradual de poder adquisitivo. Al igual que los ahorros, que en caso de no encontrarse invertidos en vehículos financieros que den como mínimo esas rentabilidades también se verán erosionados.

En el largo plazo, si no tenemos inversiones realizadas y nuestro salario no se revaloriza según el IPC, perdemos poder adquisitivo.

La deflación sería el ejemplo opuesto. Con el paso del tiempo, los costes de los bienes y servicios caen y, por tanto, nuestro dinero nos permite comprar más.

Esto parece una situación ideal. Pero lo cierto es que la deflación se relaciona con economías estancadas o decrecientes. La caída de precios vendría provocada por una caída de la demanda. Si se demandan menos bienes, las empresas reducen sus beneficios. Si los reducen, para vender más tendrán que seguir bajando precios y despidiendo personal.

Todo esto es teoría económica tradicional. En realidad, en economía no hay una causa-efecto tan clara. Tengamos en cuenta que son millones de factores los que intervienen en la economía y no se pueden simplificar con: si sucede A, entonces B.

Si fuera así de fácil, no tendríamos crisis cada cierto tiempo, o los estímulos de los bancos centrales funcionarían.

En efecto, estamos afirmando que no funcionan. No lo decimos nosotros, lo dicen los hechos.

Existen escuelas de pensamiento económico que argumentan que la inflación es consecuencia de la creación de nuevo dinero. Cuando se imprime nuevo dinero, el que está en circulación pierde valor, queda diluido. La inflación se produce cuando este nuevo dinero llega a la población, porque cada billete de hoy representa un poco menos sobre el total de dinero existente.

#### ***4.3.1. Inflación en las criptomonedas***

Hemos visto que en una economía la inflación consiste en el aumento de precios general de bienes y servicios. O el aumento de masa monetaria sin que la

economía subyacente aumente su capacidad productiva. Da igual en qué sentido queramos verlo, lo importante es saber que la consecuencia es la pérdida de poder adquisitivo. Cada vez hace falta más dinero para mantener el poder adquisitivo.

En el mundo de las criptomonedas podemos estudiarlo muy fácilmente si lo planteamos solo en términos de creación de monedas, ya que se sabe cuál es el suministro total de moneda existente y el ritmo de creación de nuevas monedas.

Vamos a considerar que la capitalización de mercado permanece constante. La capitalización es el número de monedas en circulación por el precio actual.

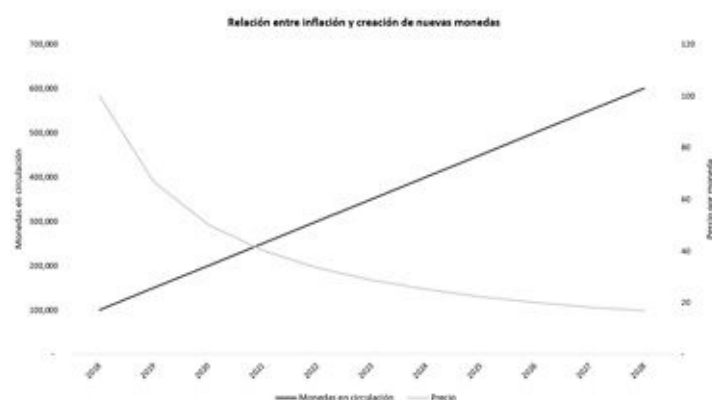
Vamos a utilizar una criptomoneda inventada:

Número de monedas en circulación = 100.000

Número total de monedas existentes = 600.000

Nuevas monedas por año = 50.000

Capitalización total (constante) = 10.000.000 €



*Fuente: Elaboración propia*

Vemos lo siguiente. El circulante aumenta a un ritmo de 50.000 monedas al año (son las nuevas monedas creadas para pagar a los mineros). Como la capitalización hemos dicho que permanece constante, significa que cada moneda nueva que se crea diluye a las que ya están creadas, porque cada vez más monedas representan el mismo trozo de pastel. Es decir, cuantas más monedas en circulación, menos vale cada una. Si mantuviéramos diez años en cartera 1.000 monedas pasaría lo siguiente:

En 2018 tenemos: 1.000 monedas / 100.000 monedas en circulación = 1% del total. Como la capitalización son 10 millones de euros, tenemos 100.000 euros.

En 2028 tenemos: 1.000 monedas / 600.000 monedas en circulación = 0,166% del total. La capitalización sigue siendo de 10 millones de euros, por lo que el valor de nuestra cartera será de 16.667 euros. Hemos perdido el 83% de nuestra inversión.

Y esta es la inflación anual según este esquema de creación de nuevas monedas:

|                               | 2018    | 2019    | 2020    | 2021    | 2022    | 2023    | 2024    | 2025    | 2026    | 2027    | 2028    |
|-------------------------------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|
| <b>Monedas en circulación</b> | 100.000 | 150.000 | 200.000 | 250.000 | 300.000 | 350.000 | 400.000 | 450.000 | 500.000 | 550.000 | 600.000 |
| <b>Inflación</b>              | –       | 50%     | 33%     | 25%     | 20%     | 17%     | 14%     | 13%     | 11%     | 10%     | 9%      |

Ahora vamos a ver el mismo ejemplo, pero en lugar de crearse un número

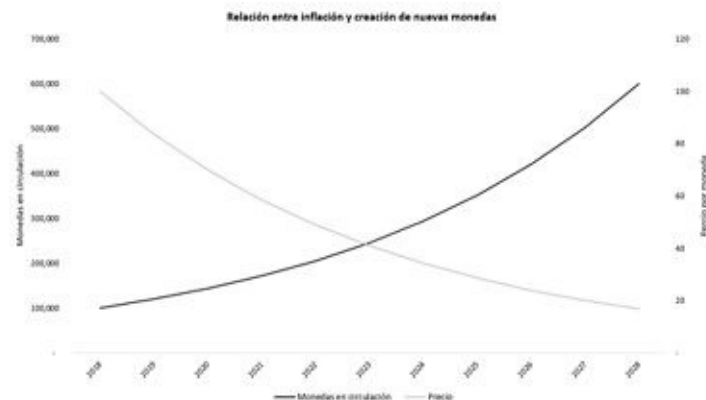
determinado de monedas al año, se creará un porcentaje sobre el total de monedas existentes y se repartirá como recompensa a los mineros:

Número de monedas en circulación = 100.000

Número total de monedas existentes = 600.000

Nuevas monedas por año = 19,63% sobre el circulante (utilizamos este valor para alcanzar en 2028 el suministro total de 600.000 monedas)

Capitalización total (constante) = 10.000.000 €



*Fuente: Elaboración propia*

Si la comparamos con la gráfica anterior, vemos cómo la curva es más suave los primeros años, y se acaban igualando en el 2028.

En Bitcoin tenemos muy claro cuál es el esquema de suministro de la moneda. Podemos saber de antemano cómo se va a diluir nuestra participación en la red con el paso del tiempo.

Ahora pensemos en nuestra economía tradicional. ¿Cuántos euros hay en circulación? ¿Cuántos billetes se imprimen? ¿Cuál es el valor total de la

economía que representan?

En el mundo de las criptomonedas hay una cosa clara. El esquema de creación o distribución de monedas es transparente desde el principio. Cualquier participante tiene la misma información que los demás. Aunque esto no significa que no pueda sufrir una modificación a futuro si la comunidad lo desea.

#### **4.4. Criptomonedas más importantes**

Vamos a hacer un repaso rápido de las criptomonedas que a día de hoy tienen más relevancia, ya sea por capitalización o porque consideremos que han jugado un papel importante en el desarrollo de la comunidad o crecimiento de los mercados. Ya hemos hablado extensamente de Bitcoin y Ethereum. Ahora vamos a conocer otros cryptoactivos muy interesantes.

##### **■ Ripple (XRP)**

Empezamos con una criptomoneda muy polémica. ¿Os acordáis de Jed McCaleb, fundador de Mt. Gox? Es uno de los fundadores de Ripple<sup>[39]</sup>. Este proyecto nació en 2011 con el objetivo de ser una plataforma de pagos transfronterizos, que no dependiera de los mineros. Las cosas no fueron muy bien entre McCaleb y la empresa, por lo que este la abandonó al poco tiempo.

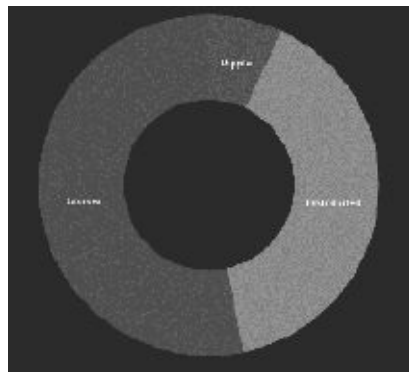
Lo primero que queremos aclarar es que Ripple es la compañía, el token es XRP. Se anuncian como la única blockchain de empresa para pagos globales.

Ripple creó el XRP en 2012, 100 mil millones, de los cuales los creadores se quedaron con 20% y dieron el 80% restante a la compañía. Desde la compañía van repartiendo estos tokens a sus clientes, pero a finales de 2018 mantienen más de 50 mil millones en su cuenta.

Eso podría suponer un serio problema para la salud del sistema económico.

Casi el total de la moneda está bajo en control de la empresa o fundadores. ¿Qué pasa si deciden vender todo? ¿O cortar el suministro para hinchar el precio artificialmente?

A finales de 2017, Ripple creó una cuenta donde depositaron los 55 mil millones que tenían en aquel momento en su poder, de tal forma que cada mes se liberarían mil millones para utilizarlos si fuera necesario. Podría tratarse de un paliativo, pero no es una solución definitiva a la concentración de poder en manos de la empresa.



*Fuente: <https://ripple.com/xrp/market-performance/>*

Esta imagen está extraída de la propia web de la compañía. Ripple tiene en su poder el 60% del suministro total de la moneda, y a fecha 26 de agosto de 2018,

tienen 7 mil millones de los 39.600 millones en circulación. Es decir, tienen casi 18% del circulante.

Aparte, Ripple como compañía ofrece tres soluciones empresariales, llamadas xCurrent, xRapid y xVia. La única que usa el token XRP es xRapid.

La compañía ha sido acusada repetidas veces de no ser transparente en sus comunicaciones. Cuando la compañía anunció que más de cien bancos estaban probando sus soluciones, lo que no especificaron es que no utilizan XRP, sino xCurrent, que es un software para liquidación de pagos transfronterizos.

Estas comunicaciones poco claras se han visto como intentos de manipulación del precio de la criptomoneda, ya que los mercados reaccionan con bastante fuerza ante este tipo de noticias. Y dado que tienen en su poder una cantidad sustancial de XRP, puede tener incentivos económicos para este tipo de comunicaciones ambiguas.

## ■ EOS

La siguiente de la que vamos a hablar es de EOS. Nace como una plataforma similar a Ethereum, donde se pudieran desplegar dApps, con el objetivo de dar solución a las limitaciones que sufre la primera en cuanto al número de transacciones. Recordemos que Ethereum se ha visto congestionada en momentos puntuales como lanzamientos de ICO, que han provocado que las transacciones tarden horas en realizarse.

EOS es una red ideada por Dan Larimer. Es una persona muy activa en el sector del blockchain. Entre sus logros están las plataformas de BitShares y Steemit, y

el haber creado el algoritmo de consenso *delegated Proof of Stake* (dPoS). En EOS funciona de la siguiente forma:

Existen 21 propagadores de bloques, elegidos por la comunidad y con una reserva de otros 100 por si alguno cae o se comporta maliciosamente. Estos propagadores son los encargados de proponer el bloque a incluir, comprobar que se ajusta a las especificaciones y anexarlo a la cadena.

Se sacrifica descentralización a cambio de mayor capacidad de procesamiento de operaciones. El eterno dilema de las blockchains públicas hasta que aparezcan soluciones de escalabilidad suficientemente seguras.

Una de las principales preocupaciones del creador era mejorar la experiencia del usuario. Para ello decidió que las operaciones en la red no estarían sujetas a comisiones. Existe una inflación anual para recompensar el trabajo que hacen los propagadores.

Es un sistema interesante. Todo poseedor de tokens soporta el coste de mantener la red en funcionamiento, independientemente del uso que haga de ella. Porque esta inflación erosiona poco a poco el valor de los tokens que se mantienen en cartera. A cambio, la usabilidad mejora sustancialmente. Al realizar una transferencia no te tienes que preocupar de conceptos como el gas en Ethereum, ni de que una transacción en un momento dado puede costarte mucho más debido a que la red se encuentra saturada.

En EOS los propagadores de bloques reciben una recompensa en forma de nuevas monedas. Con el paso del tiempo, el número total de monedas de la red crece.

Imagina que tienes en tu wallet a día de hoy 1.000 tokens de EOS. Y que el

suministro total de moneda fuera de 10.000. Por tanto, tienes  $1.000/10.000 = 10\%$  del total de tokens de la red. Van pasando los años, sigues con tus 1.000 tokens en cartera, pero ahora el suministro total de moneda ha aumentado poco a poco por las nuevas monedas creadas que han ido a manos de los propagadores de bloques. Ahora posees  $1.000/20.000 = 5\%$  del total de tokens existentes. Si en ese espacio de tiempo el valor total de la red siguiera siendo el mismo, habrías perdido la mitad del dinero. O, dicho de otra forma, has subvencionado los costes de la red mediante la inflación.

La ICO de EOS ha sido hasta el momento la que más ha recaudado en la corta historia de este sector. Consiguió recaudar la asombrosa cifra de 4.200 millones de dólares. Esto la sitúa en una posición muy fuerte para competir, ya que puede utilizar ese dinero para incentivar a los desarrolladores a pasarse a su blockchain en lugar de hacerlo en otras.

## ■ Stellar (XLM)

Stellar es, al igual que Bitcoin, una blockchain con el fin de ser utilizada para transferir valor entre usuarios. La moneda se llama lumens, y su ticker es XLM.

Nace en 2014, cuando Jed McCaleb y Joyce Kim hacen un fork del protocolo de Ripple. Utiliza un algoritmo de consenso similar al dBFT (tolerancia delegada ante fallo bizantino). Recordemos que McCaleb fundó Ripple y se fue por los continuos desacuerdos con el resto de directivos.

El objetivo con el que nace Stellar es el de interconectar sistemas de pagos, bancos y usuarios, para que se puedan realizar transferencias con unos costes mínimos. Para ello se apoya en su token nativo, el lumens, y en *anchors* (los

explicaremos a continuación).

Stellar es una red descentralizada de nodos, cualquier persona puede descargar el software y actuar como un nodo más. Así tendría una copia de la base de datos con las operaciones que han sucedido hasta entonces. Cada nodo se comunica con los demás cada 2-5 segundos, por lo que las transacciones tienen una velocidad relativamente alta.

Los anchors que hemos mencionado pueden ser bancos, empresas de procesamiento de pagos y otras entidades confiables. Actúan como puente entre las monedas tradicionales y la red de Stellar. Veámoslo con un ejemplo:

Alicia quiere enviar a Bruno 100 euros. Alicia se encuentra en España y Bruno en EEUU. Alicia utiliza la red Stellar para enviar este dinero. El sistema automáticamente busca la mejor tasa de cambio para convertir esos euros en dólares. Este intercambio lo realiza a través del token nativo, el lumens. Esta transacción se lleva a cabo casi instantáneamente, no como las transferencias internacionales tradicionales que pueden llevar días o semanas.

Ahora bien, ¿es una criptomoneda totalmente descentralizada como Bitcoin? No, ya que requiere de los anchors, donde el usuario tiene que tener una cuenta para poder sacar el dinero fiat que acaba de recibir. A no ser que los usuarios se transfieran entre sí lumens, que en ese caso sería similar a BTC. Recordemos que los anchors podrían actuar de censores de forma arbitraria, y podrían bloquear el acceso a los fondos de cualquier persona.

Las transacciones en esta red tienen una comisión ínfima, con el fin de evitar ataques del tipo spam.

## ■ Litecoin

Litecoin fue creada por Charlie Lee, una persona muy activa en el mundo de las criptomonedas y exingeniero de Google. Su visión es que, si el bitcoin era el oro del mundo de las criptomonedas, actuando como reserva de valor, litecoin sería la plata, que permitiera el pago de los pequeños gastos del día a día. Existe desde octubre de 2011.

Esta criptomoneda está basada en el código de Bitcoin, pero con algunos cambios técnicos:

- ▶ Se redujo el tiempo de minado de 10 minutos a 2,5 minutos.
- ▶ Aumentó el suministro total de moneda hasta los 84 millones.
- ▶ Algoritmo PoW intensivo en memoria.

El algoritmo de prueba de trabajo de Litecoin es conocido como Scrypt. Pretendía ser resistente a los ASIC. Es decir, que no hubiera equipos de minado altamente especializados. Esto es debido a que con estos equipos se tiende a centralizar el poder de minado en pocos actores, y Charlie Lee quería huir de esto a toda costa. Se supone que, con un algoritmo resistente a los ASIC, el minado estaría más democratizado y al alcance de cualquiera. Con el paso de los años, se han conseguido crear unos ASIC para minar Litecoin.

Recordemos que no existe ningún algoritmo resistente a los ASIC, básicamente eso sería decir que no se podría crear una máquina especializada en realizar los cálculos de forma más eficiente que una pieza de hardware genérica tipo CPU o GPU.

## ■ Cardano (ADA)

Se trata de una plataforma para Smart contracts, al igual que Ethereum y EOS, buscando dar solución al problema de escalabilidad sin que se reduzca la seguridad de la red. Y lo hacen con una filosofía científica.

El desarrollo del protocolo lo hacen basándose en investigaciones académicas revisadas por pares (*peer review*). Este proceso es el que siguen los estudios científicos antes de ser publicados. Expertos del tema revisan la información del documento y valoran la calidad del trabajo. Es una forma impedir que trabajos de dudosa calidad lleguen a ser publicados y que la comunidad científica tenga certeza de que han pasado por un riguroso análisis, y los puedan tomar como referencia para estudios posteriores.

El artífice de este proyecto es Charles Hoskinson, que a su vez fue cofundador de Ethereum. El desarrollo inicial no estaba basado en un whitepaper, sino en una serie de principios y de mejores prácticas para conceptualizar el proyecto y, a partir de ahí, crear el documento.

Cardano utiliza un algoritmo PoS llamado Ouroboros. Este mecanismo de consenso, en lugar de mineros depende de validadores. En el caso de Cardano, se selecciona un nodo para generar un nuevo bloque con una probabilidad proporcional al *stake* (participación) que tiene. Solo los *stakeholders* podrán ser elegidos para generar un bloque. El nodo seleccionado se conoce como *slot leader*. Este podrá entonces agregar las transacciones difundidas por el resto de nodos, creará un bloque, y lo sellará con su clave privada antes de transmitirlo a la red.

## ■ IOTA

Según la propia web de IOTA:

*IOTA es una revolucionaria solución para transacciones y transferencias de datos para el IoT (Internet de las cosas). Está basada en una nueva tecnología de contabilidad distribuida, el Tangle, que supera las ineficiencias de las blockchains actuales e introduce una nueva forma de alcanzar consenso en un sistema entre pares. Usando IOTA, por primera vez, las personas y las máquinas pueden transferir dinero y/o datos sin comisiones, en un entorno sin confianza, sin permisos y descentralizado. Esto significa que incluso los nano-pagos pueden hacerse sin ningún intermediario confiable.*

Lo primero que nos llama la atención es que no utiliza una blockchain, sino un sistema de contabilidad distribuida llamado Tangle (se traduciría como maraña). Es una estructura de datos conocida como Directed Acyclic Graph (DAG).



Tangle (Directed Acyclic Graph)

Básicamente lo que necesitamos saber de IOTA es que cada nueva transacción requiere que se confirmen dos transacciones previas mediante una PoW sencilla, de esta forma no se requieren mineros especializados para securizar la red.

Cuantas más transacciones haya, más rápido se confirmarán las nuevas.

Ahora bien, IOTA parece una buena idea, pero tiene una serie de problemas que necesitan ser tratados con cuidado. Actualmente existe la figura del Coordinador, que es un sistema que protege a la red de ciertos tipos de ataques mientras el volumen de transacciones no alcance una masa crítica. Es necesario que este sistema desaparezca cuanto antes, ya que debido a un problema informático dejó las carteras oficiales inaccesibles durante un par de días. Un sistema descentralizado no podría estar caído. En cambio, un sistema que tenga un punto de fallo único será atacado tarde o temprano.

El segundo problema es una vulnerabilidad mayor. El equipo diseñó su propia función criptográfica. Desde la comunidad criptográfica recomiendan que se usen sistemas existentes y testeados, porque los que hay son suficientemente resistentes y cubren las necesidades de los proyectos. Crear uno de cero es exponerse a fallos que pueden destruir el protocolo.

Un equipo de investigadores del MIT descubrió<sup>[40]</sup> una vulnerabilidad en la función criptográfica utilizada por el equipo, llamada Curl. Lograron que, con diferentes entradas, el algoritmo diera el mismo resultado (este fenómeno se llama colisión). Si la función criptográfica tiene este fallo, es factible romper las firmas de los bloques, y hacer que operaciones irregulares sean validadas. A pesar de que el equipo de IOTA corrigió esta vulnerabilidad gracias al trabajo del equipo del MIT, no gestionaron el problema de forma elegante, llegando a un pequeño desencuentro en las redes contra estos investigadores.

## ■ Tether

Esta criptomoneda tiene el objetivo de ser una stablecoin, su función es mantener un valor constante respecto a otro activo, como el dólar, el euro o el oro. Se supone que cada tether en el mercado está respaldado por un dólar americano<sup>[41]</sup>, de tal forma que, si se emiten más tether, más dólares se mantendrían en reserva para que siga habiendo paridad 1:1.

La razón por la que existen este tipo de criptomonedas es la siguiente. Imaginemos que operamos una cartera en un exchange como Binance, que a día de hoy no aceptan fiat (euro, dólares, libras, yuanes, etc.). Pensamos que va a haber caídas en el mercado y queremos protegernos contra ellas. Tendremos que pasar todas nuestras criptomonedas a alguna de las más aceptadas, como BTC, LTC o ETH. Ahora tendremos que enviarlas a otro exchange que acepte fiat, para poder vender la criptomoneda y obtener a cambio dólares o euros. Por tanto, tenemos que:

1. Vender toda nuestra cartera por alguna de las criptomonedas más comunes.
2. Enviarla a otro exchange.
3. Venderlas para conseguir fiat.

Muchos pasos, tiempo y comisiones de por medio. Y depende del tamaño de la cartera puede que tardemos días o semanas en sacarlos del exchange.

En cambio, si hacemos lo mismo utilizando una stablecoin, en este caso tether (USDT), venderíamos toda nuestra cartera por USDT y la dejaríamos en el exchange, estando expuestos a una mínima volatilidad, y preparados para cuando quisiéramos volver a comprar.

Esta criptomoneda tampoco está exenta de polémica. Parece ser que es una

compañía hermana de Bitfinex, el famoso *exchange* al que robaron 120.000 BTC<sup>[42]</sup>.

El problema que hay con Tether (la compañía) es el siguiente. Pueden generar más tether cuando quieran, con ellos comprar bitcoins, venderlos y cambiarlos por fiat. Con ello consiguen dos cosas, por un lado, aumentar el volumen de trading y precio en Bitfinex, y por otro, imprimen su propia moneda y la cambian por dinero tradicional. Además, en su propia web dicen que no tienen la obligación de cambiarte los tether por dólares.

El año pasado anunciaron que iban a auditar sus cuentas para demostrar que tras cada tether había un dólar depositado en una cuenta, y poco tiempo más tarde emitieron un comunicado en el que despedían al auditor<sup>[43]</sup>.

Resumiendo, tether es una criptomoneda muy útil para evitar la volatilidad del mercado, pero existen posibilidades de que manipulen el mercado para el beneficio propio. Habrá que ver si mejoran las prácticas de transparencia para dejar claro si realmente tienen los tether respaldados por dólares, y para asegurar que no incurrir en prácticas de crear tokens de forma irregular para cambiarlos por dólares.

## ■ Monero (XMR)

Esta criptomoneda tiene como objetivo ser totalmente anónima e intrazable. No podemos saber el origen ni destino de las transacciones, ni el balance de las cuentas. Se pretende así evitar que nadie tenga controladas sus operaciones ni se pueda conocer su riqueza. Recordemos que cada bitcoin existente es trazable desde su creación hasta el momento actual. Esto permitiría que hubiera bitcoins

«marcados». Imaginemos que una conocida agencia de inteligencia está siguiendo la pista a un peligroso delincuente, y han averiguado que este tipo tiene una cartera de bitcoins y conocen la dirección. Pueden monitorizar los movimientos de esta cartera y ver hacia dónde van los pagos y de dónde los recibe. Imaginad que por error realiza una transferencia hacia nuestra cuenta, y esa cuenta la tenemos unida a nuestro nombre porque aceptamos donaciones. ¿Quién va a aparecer en nuestra puerta a no mucho tardar?

Con Monero es imposible hacer esto y cada XMR en circulación es exactamente igual a todos los demás y, por tanto, no se puede comprobar de dónde ha venido.

Es un error común pensar que Bitcoin es anónimo e intrazable. Cuando creamos una cartera, nadie puede saber que nos pertenece. Pero en el momento en el que hagamos una operación se nos podrá relacionar con ella. Y, por tanto, las personas que puedan establecer esa relación podrán ver nuestro histórico de operaciones.

Monero logra esta privacidad mediante *ring signatures* y *direcciones secretas*. Las ring signatures o firmas en círculo es un tipo de firma digital que la puede haber hecho cualquier miembro de un grupo, sin que pueda determinarse quién ha sido.

Expliquémoslo con más detalle:

Cuando quieres hacer una transacción, tienes que firmarla con tu clave privada para que pueda ser realizada. Esto evita que cualquier persona que no tenga la clave pueda retirar tus fondos. Pues bien, se combina en un grupo tanto al firmante de la operación como a varios no firmantes. Estos provienen de transacciones pasadas. Lo que se ve desde fuera es que la transacción la podría

haber realizado cualquiera del grupo, porque todas aparentemente son válidas. Lo que ha sucedido es que se ha combinado la transacción que estamos haciendo con varios señuelos, para que no se pueda determinar origen y destino de fondos.

Y las direcciones secretas funcionan de esta forma:

Todo el mundo posee una clave pública, que es la que comparte para poder recibir transacciones. Si queremos enviar fondos a una persona y nos da su clave pública, la transacción se realizará a una dirección recién creada de un solo uso utilizando dicha clave. Esa dirección pública no quedará grabada en la blockchain. El receptor tendrá que usar su *view key* para escanear toda la blockchain, y comprobar cuántas transacciones ha recibido para saber qué fondos tiene disponibles.

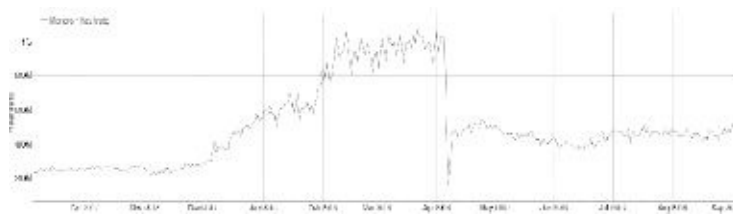
Con estas dos técnicas Monero consigue ocultar la dirección del que hace el envío (*ring signatures*) y oculta la dirección del receptor (*stealth address*).

Monero utiliza un sistema de prueba de trabajo. En la comunidad se sospechaba que actores como Bitmain, el principal fabricante del mundo de equipos de minado ASIC, habían sido capaces de desarrollar equipos para minar Monero.

Recordemos que se considera que los ASIC facilitan la centralización. Esto es debido a las economías de escala. Un actor con suficiente dinero puede comprar equipos directamente al fabricante y negociar electricidad más barata. Esto le coloca en una situación de ventaja que hace que gane proporcionalmente más dinero que un individuo. Y cuanto más dinero gane, más ventaja puede seguir sacando a los competidores. Así que con Monero se tomó la decisión de modificar el algoritmo de tal forma que estos equipos, en caso de existir, quedaran obsoletos. Al estar tan especializados en una tarea concreta, en cuanto

se modifica ligeramente el algoritmo de prueba de trabajo esos equipos dejan de servir.

Una vez que la comunidad decidió implementar estos cambios se notó una gran caída en el hashrate de la red de Monero. En la imagen siguiente se puede ver la magnitud del cambio.



*Fuente: <https://bitinfocharts.com/comparison/monero-hashrate.html#1y>*

Tras la actualización del algoritmo, ¡el 80% del hashrate desapareció! Según los mineros fueron actualizando el software, parte de ese hashrate se recuperó, quedando entorno al 50% del hashrate previo al cambio. Esto es una clara señal de que había equipos ASIC minando en la red de forma oculta. A Bitmain ya se le había acusado de meter equipos en la red a minar meses antes de comercializarlos. Parece que podría ser así (por parte de ellos o de otros competidores), ya que nadie había anunciado mineros para Monero. En cualquier caso, parece que esto seguirá sucediendo de forma esporádica en el futuro, y cada cierto tiempo la comunidad votará si actualizar el algoritmo o no para dejar obsoletos los nuevos ASIC desarrollados.

En este caso que vemos, si realmente todos los equipos pertenecían a la misma empresa, el riesgo que existía de un ataque malicioso era real. Controlando un porcentaje tan alto de la capacidad de minado de una red, se pueden censurar

operaciones, elevar las comisiones de la red o incluso ejecutar operaciones de doble gasto.

## ■ **Binance Coin (BNB)**

Este token es uno de los que consideramos más interesantes a día de hoy. Fue creado por el exchange Binance mediante una ICO. En el [whitepaper<sup>\[44\]</sup>](#) se exponían las dificultades de las plataformas de trading de criptomonedas en aquel momento:

- ▶ Arquitecturas técnicas pobres.
- ▶ Plataformas inseguras.
- ▶ Poca liquidez.
- ▶ Servicio de atención al cliente de mala calidad.
- ▶ Poca internacionalización.

El CEO de Binance, Changpeng Zhao, cuya vida profesional había estado dedicada a la creación de sistemas de trading, veía una oportunidad única en crear la mejor plataforma de intercambio en el mundo de las criptomonedas. Y así fue, ya que, en solo unos meses, Binance se convirtió en el exchange más utilizado del mundo.

Durante la ICO se crearon 200 millones de BNB. 100 millones destinados al público participante, 80 millones para el equipo fundador, y 20 millones para *angel investors*. Cada trimestre Binance recompra tokens dedicando un 20% del beneficio de ese periodo para destruirlos. De esta forma, con menos tokens en

circulación, los poseedores de tokens verían cómo se incrementa el valor de los que guardan en cartera. Es como la recompra de acciones de una empresa tradicional. Van a seguir haciéndolo hasta dejar en circulación solo 100 millones de BNB.

Poseer el token otorga otra ventaja al usuario de la plataforma. Las comisiones de trading tenían un descuento del 50% el primer año, 25% el segundo, 12,5% el tercero, y 6,75% el cuarto si se pagan estas comisiones utilizando el BNB.

Por último, la intención de Binance es crear un exchange totalmente descentralizado, es decir, que funcione sin intermediarios. El BNB también será usado aquí para pagar las comisiones y costes de la plataforma.

Tras este repaso a algunas de las criptomonedas que consideramos más relevantes a día de hoy, vamos a pasar a explicar un mecanismo de financiación que, en parte, explica la explosión que ha habido en cuanto a número de proyectos relacionados con blockchain durante el 2017.

## **4.5. Qué es una ICO**

Tal y cómo hemos visto, blockchain es una tecnología disruptiva y ha cambiado radicalmente las prácticas habituales en algunos sectores.

Esto es cierto hasta tal punto que ha creado una nueva forma de financiación, llamada ICO (Initial Coin Offering) y es una fórmula bastante parecida al crowdfunding.

Una ICO consiste en captar fondos. Se intercambian activos digitales (un token) por las criptomonedas más comunes, normalmente BTC y ET. Y aunque hay países en los que se han llegado a prohibir, por lo general cualquier persona podía participar en ellas, independientemente de su edad, conocimientos, etcétera.

Es un mecanismo muy innovador ya que se consiguen dos cosas de forma rápida:

1. Se logra financiación sin tener que ceder capital de la empresa.
2. Se distribuye la criptomoneda o el token a nivel mundial entre potenciales usuarios.

Pensemos que las primeras ICO que tuvieron lugar las lanzaron personas que llevaban años involucrados en el espacio blockchain. Proyectos muy innovadores, con alto potencial y formado por los mayores expertos. Mediante la distribución del token a cambio de dinero, se conseguía que solo las personas más interesadas tecnológicamente en el desarrollo se implicaran en las fases tempranas de la vida del proyecto, y a su vez se creaba una comunidad que soportaría el de la red. ¿Quién se iba a involucrar en una idea aún no testada, pagando, sino los más devotos del ecosistema blockchain?

Esta comunidad sería la encargada de probar en real el funcionamiento de la red, ayudar a mejorar el protocolo en caso de encontrar fallos, e ir creciendo en hashrate poco a poco. De esta forma, los desarrolladores son capaces de ir viendo si el proyecto se desarrolla acorde a sus planteamientos iniciales.

Y, en efecto, este tipo de financiación ha dado muy buenos resultados. Estos

pioneros lanzaron sus proyectos y consiguieron que los *early adopters* obtuvieran rentabilidades increíbles, hablamos de incluso más del 100.000%, como es el caso de Ethereum.

Con el paso del tiempo esta fórmula ha llamado mucho la atención dentro y fuera de la comunidad. Cada vez más proyectos copiaban este método, incluso aunque su idea no tuviera relación con blockchain se le añadía para poder financiarse mediante este mecanismo. Hay una cantidad increíble de proyectos que utilizan token sin que realmente sea necesario.

Y se ha convertido en un espacio muy peligroso.

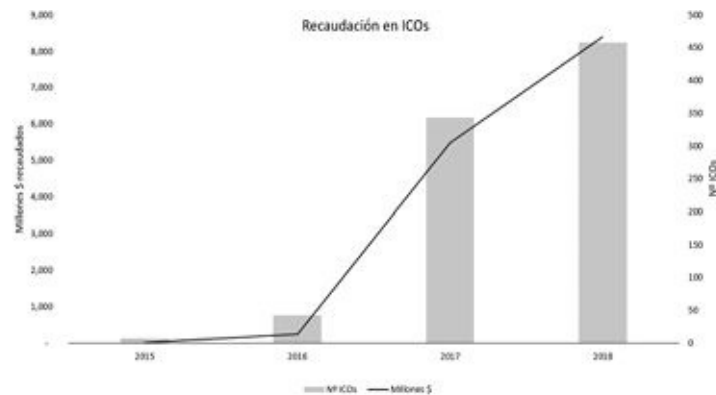
¿Una fórmula para captar dinero, sin ceder propiedad de la empresa, y sin control regulatorio?

Imaginaos lo que ha pasado.

De ver el lanzamiento de una ICO o dos al mes, a cientos todos los meses. Y recordemos el estado del arte actual. Estamos hablando de una tecnología puntera, para la que aún existe muy poca capacitación a nivel mundial. Los mejores expertos ya están involucrados en proyectos importantes.

En una ICO cada vez tiene más importancia la parte de marketing que la parte tecnológica que hay detrás. Esto, obviamente, no conduce a ningún lugar, y cuando los equipos intentan desarrollar el proyecto se dan cuenta que no tienen las capacidades o que han sido demasiado optimistas en sus previsiones y terminan por abandonarlo. Pero después de haberse embolsado cantidades astronómicas. Idealmente, una ICO se lanzaba cuando el proyecto se había desarrollado bastante y se había comprobado que era tecnológicamente viable. Ahora se lanzan con solo la idea en papel, y la mayoría de equipos no son

capaces de llevar las ideas a buen puerto.



*Fuente: Elaboración propia*

Como podemos ver, durante 2018 (incluyendo hasta agosto) se han lanzado más ICO que en todos los años anteriores. Es muy difícil de saber cuántas son capaces de desarrollar su proyecto hasta poder lanzarlo, pero la realidad es que muchos equipos dejan de publicar en redes sociales y sus webs dejan de hacer actualizaciones. Incluso muchos miembros pasan a trabajar en otros equipos. Esto hace que sea muy arriesgado invertir en una ICO sin estudiarla a fondo o conocer al equipo.

## 4.6. Cómo analizar una ICO

A la hora de analizar una ICO hay que ser muy crítico, ya que se puede perder el dinero fácilmente. Al tratarse de una actividad aún no regulada, están sucediendo muchos abusos e incluso timos.

Vamos a intentar dar unas pautas generales para que el lector pueda invertir en aquellos proyectos que considere que son dignos de su atención y su dinero.

Lo primero que recomendamos hacer es leer el whitepaper. Este es un documento técnico que tiene como finalidad exponer un problema, y explicar cómo se le va a dar solución. Normalmente es un documento complejo, ya que hablamos de que va a solucionar un problema existente mediante una capa de tecnología basada en blockchain. Aunque sea difícil de entender, realmente está al alcance de todo el mundo distinguir entre un documento bien elaborado y al que se le ha dedicado mucho tiempo, de uno escrito rápidamente y con intención de captar clientes. Es interesante consultar las fuentes que citan (si es que lo hacen), ya que podemos tener una idea más clara de la formación que tienen en el área en cuestión.

Una vez leído el whitepaper, ya deberíamos tener una idea clara de qué se está proponiendo y si parece alcanzable. Objetivos demasiado ambiciosos o que se basan en hipótesis no validadas pueden dar idea de un optimismo irracional.

Ahora que ya sabemos que quiere hacer, tenemos que pensar:

¿Necesita usar tecnología blockchain? ¿Por qué? ¿Qué función cumple la criptomoneda o token? ¿Cómo se incentiva su uso, y cómo de realista es el planteamiento?

Dado que estamos en un momento en el que captar capital a través de una ICO es muy sencillo, han aparecido muchos actores oportunistas que ven la forma de financiar su negocio tradicional de esta forma. Sin diluir su participación en una empresa, sin tener que devolver el dinero, sin tener que cumplir la regulación... Es la mezcla perfecta para que cualquier persona incluya blockchain sin ser

necesario, solo para poder lanzar el proyecto utilizando esta fórmula.

También tendríamos que ser capaces de saber en qué fase se encuentran. ¿Es solo conceptual? ¿Tienen alguna versión mínima del producto en fase de testeo? ¿Cuánto tiempo llevan trabajando en ello?

A continuación, podemos pasar a echar un ojo a la web. Es interesante ver la estructura que tiene, y se suele explicar la tecnología de forma más sencilla que en el whitepaper (y más atractiva, utilizando imágenes o infografías). La web es la cara pública del proyecto, y lo ideal es que el detalle esté totalmente cuidado y haya coherencia entre los contenidos.

Es habitual también publicar quiénes son los miembros del equipo. Dedicemos un buen rato a esto. Hay que investigar a todos uno a uno, es una actividad tediosa pero totalmente necesaria. Es muy fácil detectar engaños si cumplimos con esta fase.

¿Tienen experiencia en su puesto?

¿Son personas conocidas en su campo?

¿Trabajan a tiempo completo en este proyecto?

¿Existen sus perfiles sociales?

¿Encontramos referencias a ellos en los buscadores?

Tenemos que ser capaces de entender por qué cada persona ocupa el puesto que ocupa, y si es lógico que esté ahí. Además, también es muy importante la dimensión del equipo.

Imaginemos que el proyecto propone solucionar un problema con la escalabilidad de las blockchains públicas. Claman que su red es capaz de

procesar 100.000 TPS (transacciones por segundo). No tienen aún un modelo en fase de testeo que valide esta hipótesis, pero según sus cálculos técnicamente es viable, y además, el responsable de desarrollo es alguien que no tiene experiencia en este campo ni tiene un equipo de programadores a su cargo.

¿Es realista?

La respuesta es no.

Es sorprendente el número de proyectos que hacen declaraciones tan a la ligera y, de hecho, es una de las formas más fáciles de detectar proyectos que van a fallar. Proponer soluciones magníficas, no testeadas, y sin el equipo adecuado es un billete directo al fracaso.

Muchos proyectos ya se adelantan y dicen que primero captan el capital y que luego podrán desarrollar el producto. Vamos, que básicamente primero pagas por algo, y si tienes suerte y consiguen desarrollarlo, te dan una plataforma que utilizar.

¿Os suena lógico?

Además, no olvidemos que se trata de una tecnología puntera. No sabemos a ciencia cierta cuánta gente hay alrededor del mundo capacitada para desarrollar proyectos basados en blockchain, pero seguro que muchísima menos de la necesaria para la cantidad de proyectos existentes.

¿Qué pasa si necesitan contratar a un equipo de desarrolladores blockchain y no son capaces, porque los que hay ya están trabajando en proyectos que les consumen todo su tiempo?

El proyecto se muere.

Y el público que ha participado en la ICO se queda con unos tokens que no valen nada, ni valdrán nada nunca.

A día de hoy el equipo no tiene responsabilidades legales si abandonan el proyecto sin haberlo desarrollado.

Seguimos mirando la página web y llegaremos a un itinerario o *roadmap*. Esto es una serie de hitos que pretenden alcanzar y en las fechas donde estiman que lo harán. Es muy difícil estimar plazos, y normalmente son bastante agresivos. Podemos mirar en el momento que estamos y cómo han cumplido los hitos anteriores. ¿Han llegado en fecha?

Es también muy importante la comunicación que tienen con la comunidad. Las mejores prácticas consisten en informar continuamente, bien sea con artículos en un blog, a través de Twitter, Slack, o algún otro método. Si explican qué están haciendo y cómo, contando los problemas que se encuentran y los eventos en los que participan, te pueden dar una mejor idea de lo que hay detrás del proyecto.

La transparencia es fundamental, y más cuando estamos hablando de captar varios millones de euros o dólares sin dar participación en la empresa ni tener responsabilidades de ningún tipo.

Recordemos que la mayoría de tecnologías blockchain públicas son open source. Esto quiere decir que el código está disponible para que cualquiera lo vea y lo pueda utilizar. Se mantienen habitualmente en repositorios de Github, y podemos chequear fácilmente las contribuciones que hacen los desarrolladores que están trabajando en él. Si no hay actividad, mala señal, y si es un repositorio privado, hay que tener cuidado. ¿No comparten porque un competidor les puede copiar y lanzar la tecnología antes que ellos? ¿O realmente no están desarrollando nada y

lo tienen que ocultar?

A continuación, investiguemos redes sociales, tanto las de la empresa como las de los particulares. ¿Hay actividad? ¿Los particulares reflejan que están involucrados en el proyecto? ¿Son activos en eventos del sector? Con esto te puedes hacer una idea del compromiso que tienen con la comunidad y si realmente están involucrados en el proyecto o no.

Sigamos con lo demás que tenemos que mirar para invertir en una ICO.

El capital mínimo y máximo buscado, y a qué se va a destinar.

Lo ideal es que sea una horquilla realista. Si planteas un mínimo de 500.000 euros y un máximo de 50 millones... algo raro hay. ¿Con el mínimo eres capaz de desarrollar la solución y lanzarla? Si es así, ¿para qué necesitas entonces un máximo de 50 millones? No se trata de pedir dinero por pedirlo, se trata de hacer una estimación razonable para poner en marcha la solución. Si un equipo plantea que su desarrollo le costará, digamos, ese medio millón, y tiene 49 millones esperándoles en una cuenta... ¿Qué incentivo tienen para seguir trabajando? ¿Van a ser eficientes en el uso de capital? ¿Van a seguir esforzándose cuando tienen la vida prácticamente solucionada?

Y en cuanto a cómo destinar los fondos, también podemos hacernos una idea de las buenas prácticas del equipo. ¿Cuánto dinero va al equipo? ¿Cuánto a legal, a marketing, a desarrollo, a acuerdos con terceros...? ¿Y cuánto a fundadores?

Creemos que el equipo tiene que tener un buen salario para poder no preocuparse de pagar las facturas y de vivir cómodamente. Pero quedarse, por ejemplo, el 40% de una inversión máxima de 50 millones es un total abuso. Y un desincentivo de una magnitud considerable.

Hay fórmulas para minorar este factor, como bloquear los fondos a los que puede acceder el equipo en periodos de tiempo. El problema es que no implica que no los puedan sacar nunca, simplemente que tendrán que esperar unos meses o unos años. Aun así, vemos que es una solución mejor a la de no tener bloqueados los fondos, porque de esta manera el equipo tendría que luchar por que el proyecto saliera o sus tokens no valdrían nada.

Es habitual que los equipos recurran también a la figura de *Advisors*. Estas personas suelen ser expertos en una materia que prestan sus conocimientos al proyecto, o bien figuras estratégicas por alguna determinada razón.

Es fácil justificar la presencia de un experto en la materia. Pero cuando hablamos de figuras estratégicas, es más difícil evaluar su idoneidad. Esta figura estratégica lo ideal es que sea una persona que aporte valor dentro del sector. Puede ser que tenga mucho contacto con diferentes equipos, con exchanges, con medios de comunicación... Este tipo de advisor puede abrir muchas puertas para facilitarle al equipo lanzar la ICO.

Ahora bien, ¿y si estas figuras son de fuera del mundo blockchain? Deportistas, traders, cantantes...

No aportan nada de valor al proyecto. ¿Crean hype para que más gente quiera comprar la moneda? Sin duda. ¿Es gente que va a aguantar el token porque cree en el proyecto, o lo va a vender en cuanto pueda, provocando una caída en precio que, además, espante a los inversores? La respuesta parece clara.

Utilizar famosos para promocionar el proyecto con el único objetivo de recaudar dinero es un error. Sobre todo, porque suele ir dirigido a un público que no es conocedor de los riesgos de invertir en una ICO. Hay algún ejemplo de malas

prácticas utilizando este tipo de estrategias<sup>[45]</sup>.

También nos fijaremos en si hay empresas que hayan financiado el proyecto en las fases más tempranas. Es bastante habitual encontrar empresas con mucho renombre en el espacio (placeholder, #hashed, DHVC...). Esto no se puede convertir en la única razón para invertir en la ICO. No sabemos en qué condiciones han entrado, ni con cuánto capital, por lo que podemos ser partícipes de una apuesta muy arriesgada.

Para terminar, hay que fijarse en cómo se va a lanzar la ICO. Nos podemos encontrar varias fases, pero no necesariamente tienen que realizar todas. Cada equipo hace lo que considera más adecuado. A continuación, explicamos las fases que suelen darse habitualmente:

- ▶ **Private sale:** A esta venta privada normalmente solo pueden acudir inversores acreditados. Las condiciones son las más ventajosas, ya que están financiando los primeros gastos de la empresa sin que haya todavía visibilidad de cuándo puede estar listo el producto y, por tanto, reciben bonus muy altos. Es habitual que reciban descuentos sobre el valor del token del 50% o incluso más.
- ▶ **Pre-sale:** Esta es una fase creada para generar demanda y miedo de quedarse sin poder participar. Es una venta previa a la venta pública, y normalmente puede acudir cualquiera que se registre a tiempo. Es decir, una venta pública antes de la venta pública. Vaya. Tiene solamente el objetivo de crear expectación. Y los descuentos también son sustanciales, habitualmente en el rango del 20%-30%.
- ▶ **Public sale:** Esta fase es a la que cualquiera puede acudir e invertir a cambio de recibir tokens. Puede que haya descuentos para los que compren en las

primeras horas, pero no es siempre así. Aquí se ha visto de todo: desde las guerras de gas (esto es, hacer la transacción pagando una comisión muy alta para que entre en el siguiente bloque minado, y no quedarse sin participación), suplantación del sitio web, suplantación del Smart contract, etc. La expectación y las prisas son muy malas consejeras, y se han producido pérdidas multimillonarias a la hora de enviar la contribución a los proyectos.

Esta fase de venta pública a veces esta fase se llama TGE (Token Generation Event) o algún otro nombre que se les ocurra a los miembros del equipo para intentar huir de la imagen de que están ofreciendo un producto financiero a inversores no acreditados (ICO es muy parecido a IPO, lo que conocemos aquí como una OPV o salida a Bolsa de una empresa tradicional).

Por las últimas ICO que hemos visto, ahora es habitual que tengas que estar registrado para poder participar, y con una contribución máxima. Así se evitan los cientos de pérdidas económicas derivadas de enviar fondos a direcciones falsas o erróneas y las guerras de gas. Cada participante tiene reservado unos tokens durante un periodo de tiempo de varias horas o días.

El proceso de registro se conoce como *whitelist*. Y tiene una doble función. Por un lado, controlar el número de participantes y, por otro, tener datos de estos participantes por si el día de mañana las autoridades exigen a los promotores del proyecto información de estos.

En cualquier caso, una vez que la ICO ha tenido lugar, ¿qué viene a continuación?

Cuando se cierra el periodo de contribuciones, viene la espera. A veces recibimos el token al momento, a veces a los pocos días, a veces tendremos que

esperar semanas o meses, pero tarde o temprano recibiremos en nuestra cartera los tokens que hemos comprado. Una vez que los hemos recibido, podemos acudir a un exchange o a un DEX (Decentralized Exchange) y venderlos.

Lo habitual era que, tras la ICO, los tokens cotizaran con una subida asombrosa, ya que la gente que no había podido comprar quería también tenerlos. Ahora es más habitual ver caídas abismales. Y en parte es lógico, gracias al esquema cuasi-Ponzi que es favorecido por la estructura de la ICO. Si vendemos tokens a diferentes personas, a precios distintos, estamos incentivando que los que hayan comprado tokens en las primeras fases los vendan en cuanto puedan, ya que con la diferencia entre el precio de compra y el precio del público general es del doble o más incluso. Beneficio rápido y asegurado.

#### **4.7. Qué es una STO**

Las ICO han cambiado el modelo de financiación tradicional, pero conllevan una serie de desventajas para el inversor que hace que este formato pueda resultar poco atractivo para una amplia mayoría.

Cuando accedemos a una ICO compramos los tokens que nos permiten interactuar con una plataforma, pero ¿qué ocurre si la empresa decide abandonar el proyecto? La respuesta es simple, no podremos exigir nada porque solo tenemos derechos de acceso sobre la plataforma en cuestión, no sobre el resto de activos o proyectos de la compañía.

No es de extrañar que un inversor tenga preocupaciones sobre este modelo, por

lo que para encontrar un camino intermedio entre la financiación tradicional y las ICO, nacieron las STO.

Una STO, o Security Token Offering, consiste en la venta de tokens security, que son considerados como una inversión a efectos legales. Han de cumplir la legislación en materia de inversiones de cada país, por lo que se restringe en parte la facilidad para captar capitales que ofrecía una ICO, pero a cambio se da mayor garantía al inversor.

Un token security representa derechos reales sobre la empresa. Puede ser sobre el beneficio, sobre los activos, sobre el capital social, etc. De esta manera se puede tokenizar una empresa, de forma que el inversor acceda a una serie de derechos y obligaciones que no tendría si participara en una ICO. La propiedad y transmisión del token se produciría en una blockchain, con la misma facilidad con la que ahora compramos y vendemos acciones a través de un bróker.

La siguiente pregunta que nos debemos hacer es simple: ¿por qué un negocio querría realizar una STO cuando existen los métodos tradicionales de captar financiación?

Una de las ventajas principales sería ofrecer liquidez a las inversiones en empresas pequeñas. Cuando un emprendedor quiere financiar su proyecto, muchas veces está limitado a acudir a Venture Capital. Cuantas menos opciones de financiación existan, menos poder de negociación tendrá, por lo que las condiciones pueden ser muy desfavorables. Esto es en parte a que la transmisión de títulos de empresas pequeñas es muy difícil, no hay mercado suficiente.

Si se logra financiarse a través de una STO se tienen ventajas considerables como que el emprendedor puede decidir qué parte tokenizar, por ejemplo, el

beneficio, en lugar de tener que dar capital social. Además, estos tokens son transmisibles en mercados secundarios, por lo que se generaría liquidez para el inversor que quiera venderlos y la oportunidad de otra persona para comprarlos. Es una ventaja tanto para el inversor como para el emisor.

Ahora bien, en un estado tan incipiente, no es fácil lanzar una STO. Hay que cumplir con la normativa del país en cuanto a la emisión de valores. Esto implica que no cualquiera puede acudir a comprar tokens en la STO, con la limitación que eso puede suponer a la hora de conseguir el capital suficiente. Un token comprado en una ICO se puede vender en cualquier exchange, mientras que un token security no, solo en mercados secundarios regulados.

A pesar de las dificultades que puedan existir a día de hoy, las STO se pueden convertir en una forma de acercar al inversor tradicional al mundo del blockchain. La creación de estos puentes entre los sistemas habituales y las nuevas formas disruptivas son importantes para derribar barreras y que el sector evolucione más rápidamente.

## **4.8. Carteras**

En este capítulo hablaremos del lugar donde guardamos las criptomonedas que poseemos, ese lugar se conoce como cartera, monedero o wallet.

Un wallet de criptomonedas tiene como función almacenar los activos digitales que tengamos. Es un software que nos permite acceder a una dirección en la blockchain donde están nuestros fondos. Cada blockchain es distinta, tiene un formato de dirección propio y, por tanto, tiene su propia cartera. De ahí lo

complicado de todo esto. Lo más seguro es tener una cartera por cada criptomoneda que tengamos (que no sea un token de Ethereum, que son almacenados en la misma dirección), pero también exige que tengamos multitud de contraseñas y puede ser un problema.

La cartera básicamente es la dirección pública y la clave privada. Sin clave privada de nuestra cartera, nuestros fondos serán inaccesibles. Como veremos más adelante, hay diferentes tipos de wallets y cada uno de ellos tiene asociado un nivel mayor o menor de seguridad.

Al igual que con el dinero fiduciario disponemos de cuentas bancarias donde almacenarlo y poder gestionarlo de forma fácil y cómoda, con las criptomonedas tenemos la posibilidad de almacenar nuestras criptomonedas en wallets.

## ■ ¿Cómo funciona una cartera?

La clave pública podría ser nuestra dirección de correo electrónico, es decir, una dirección que compartimos con nuestros contactos y amigos y con la que podemos recibir emails. La clave privada sería nuestra contraseña, que unida a nuestra dirección nos permite poder operar con el correo, es decir, leer los mensajes que nos han enviado y enviar emails a otras personas.

Las claves privadas son códigos de 256 bits que constan de 64 caracteres que se generan de forma aleatoria o por el usuario o por algún software de ayuda como el que integran algunas wallets. Este código funciona como forma de autenticación de usuario y sirve para demostrar quién es el propietario de ese monedero. Sin este código, no se pueden firmar operaciones y, por tanto, no se podrían enviar fondos a ninguna otra dirección.

La clave privada es lo que te da poder sobre una dirección pública. Si compartes tu clave privada, o te la roban, será muy fácil que te quiten los fondos y los envíen a otra dirección para que no puedas volver a tocarlos. Por eso lo más importante es nunca compartir esta clave, y mantenerla apuntada en algún sitio muy seguro, nunca en el ordenador (por lo menos sin encriptar el archivo).

Otro dato importante es que las claves pública y privada están relacionadas entre sí de forma matemática y la clave pública deriva de la clave privada. Por lo tanto, no es necesario que guardemos ambas claves, nos valdría solo con guardar la clave privada.

Un ejemplo de una clave pública y privada de Bitcoin es la que mostramos a continuación:

Clave pública (dirección de bitcoin):



1KaabLJKY715sSexCvzG6Df3cC6cRR6uR6

Clave privada:



KymZhF3K4RqA3rHcn6NvjkcQ3kVrZHLikxZrj7XTkeyT5sbHfTVz

Como se puede ver en el ejemplo, disponemos de la dirección de la clave pública y privada, y además disponemos del código QR asociado a cada una de las direcciones (un código QR es un código de respuesta rápida, *Quick Response* en inglés) que sirve para almacenar información en una matriz de puntos o en un

código.

Si escaneamos el código QR con un software compatible, podemos ver que la información que almacena es la dirección de la clave pública o la dirección de la clave privada.

## ■ Tipos de monederos de criptomonedas

Para hacer la clasificación de los tipos de monederos de criptomonedas que existen se pueden usar diferentes modelos. Dos de los más importantes son la clasificación de los monederos como frío o caliente, y la clasificación de los monederos como determinista o no determinista.

Un monedero de criptomonedas frío o *cold wallet* es un monedero que no está conectado a la red de internet y, por tanto, hackearlo no es una opción. La seguridad de este tipo de monederos es más alta que la de los hot wallets. Hay que localizarlo físicamente para poder tener acceso a él, lo cual hace que sea extremadamente difícil de atacar.

Un monedero de criptomonedas caliente o *hot wallet*, es un monedero que está continuamente conectado a internet y tiene posibilidades de ser hackeado. Un ejemplo son los monederos online de criptomonedas.

Para saber si un monedero es determinista o no determinista tenemos que ver cómo son creadas las claves privadas que están almacenadas en el monedero.

Si todas las claves privadas del monedero parten de una misma «semilla», estamos hablando de una cartera determinista. Una semilla es un número aleatorio que se combina con otros datos y que genera diferentes claves privadas.

Gracias a tener una semilla común para generar todas las claves privadas es posible poder recuperar estas a partir de la semilla. Solo con esta semilla se podrán hacer importaciones y exportaciones del monedero. Además, se consigue que para tener una copia de seguridad de todo el monedero solo haya que guardar una clave privada.

Para algunos monederos de criptomonedas es posible generar la semilla a partir de una secuencia de entre 12 y 24 palabras. Las palabras para la secuencia son elegidas por el propietario del monedero y es una forma más fácil de disponer de una copia de seguridad más fácil de recordar. Gracias a la secuencia de palabras es posible generar la semilla del monedero y con esta semilla crear las diferentes claves privadas y públicas.

En cambio, si las claves privadas son generadas de forma aleatoria se conoce al wallet como no determinista de Tipo-0. Es decir, si el monedero tiene 100 claves privadas diferentes, al no existir una relación entre ellas tendremos que almacenar las 100 claves para poder tener acceso a los diferentes sub-monederos que tengamos en la cartera. Tendremos que hacer copias de seguridad con mayor asiduidad si queremos evitar la posibilidad de poder perder el acceso a nuestras criptomonedas.

## ■ Monederos en línea o Web Wallet

Este tipo de cartera es a la que accedemos conectándonos a una plataforma web. Normalmente se accede mediante claves sencillas. Son cómodas, pero es el tipo de cartera más vulnerable. Por un lado, nosotros no tenemos en nuestro poder la clave privada, lo cual de por sí ya es bastante malo. Si no tenemos nuestra clave

privada, la cuenta no es nuestra, así de simple. Estamos delegando en un tercero la custodia de nuestro activo. Pero es que, además, estas empresas son un blanco natural para atacantes, ya que amasan la fortuna de miles de personas.

Este es el tipo de cartera que ofrecen los propios exchanges. Cuando compramos criptomonedas en sitios como Coinbase o Kraken, se quedan almacenados en las carteras que las empresas tienen habilitadas. Suelen tener diferentes mecanismos para prevenir el robo masivo de fondos. Pero siguen siendo inseguros. Si no les roban a ellos directamente, puede que seamos nosotros los atacados mediante *phishing*<sup>[46]</sup>, o *keyloggers*<sup>[47]</sup>, o algún otro método para acceder a los fondos con nuestra clave.

### ■ Monedero de escritorio o Desktop Wallet

Son un software que descargamos en el escritorio de nuestro ordenador. Las claves privadas se almacenan en este, por lo que tienes el control total de la cartera. Por lo general, existe la versión de los desarrolladores de la blockchain, como Bitcoin Core para Bitcoin, o la Ethereum wallet de Ethereum. O de terceros como Jaxx o Exodus, que permiten almacenar varias criptomonedas distintas.

### ■ Monedero de teléfono móvil o Mobile Wallet

Exactamente igual que el monedero de escritorio. Se descarga un software en el teléfono móvil y en él se almacenan las claves privadas. Hay que tener más cuidado con este tipo porque suelen aparecer en las tiendas de Apps versiones

falsas con el objetivo de captar claves privadas y poder robar los fondos. Recomendamos utilizar solo aquellas que son oficiales o de terceros de confianza, y siempre chequear en la web oficial que realmente es una aplicación desarrollada por ellos.

## ■ Monedero físico o Hardware Wallet

Los monederos físicos son del tipo cold wallet y son la opción más segura de todas. Estos no están conectados permanentemente a la red. Solo los conectaremos al ordenador cuando queramos realizar alguna operación. Las claves privadas están almacenadas en su interior, y tendremos la posibilidad de apuntarnos una serie de palabras que generan la semilla de nuestra cartera para poder restaurarla si perdemos el dispositivo físico. Para operar se requiere interactuar con el ordenador y con los botones del propio dispositivo, por lo que es imposible sufrir ataques de forma remota.

Los más comunes a día de hoy son el Nano S de Ledger, o el Trezor One, de Trezor. Cada uno de ellos tiene sus desventajas, por ejemplo, no son compatibles con las mismas criptomonedas. En función de los activos digitales que tengamos, tendremos que elegir el que más se ajuste a nosotros.

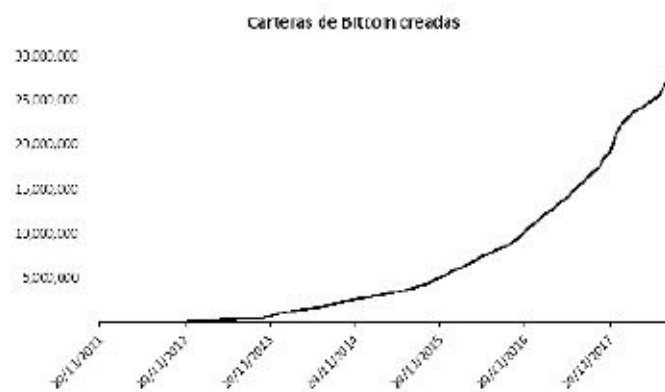
De forma generalizada, todos dejamos nuestros criptoactivos en algún exchange como Coinbase o Binance. Si estamos haciendo trading de forma diaria es cierto que poco podemos hacer. Pero si compramos y vendemos de forma esporádica, lo mejor será que saquemos los fondos de estos sitios y los enviemos a nuestras carteras personales.

Los exchanges suelen sufrir una gran cantidad de ataques diarios. Y, por lo

general, no se hacen responsables de los robos sufridos (ya que en muchas ocasiones esto les lleva a la quiebra) y los bienes no están asegurados. Sabiendo el peligro al que están expuestos nuestros activos, deberíamos de tomar las medidas posibles para protegerlos.

En el gráfico mostrado a continuación podemos observar cómo ha crecido el número de carteras de Bitcoin.

Este número solo incluye las carteras oficiales abiertas en <https://www.blockchain.com/>. Esta web nació como un explorador de bloques (donde podemos buscar cualquier dirección o transacción de Bitcoin) y proveedor de carteras, y con el paso del tiempo se han convertido en un referente en el sector. Por sus filas han pasado personas como Changpeng Zhao (CEO de Binance) o Andreas Antonopoulos (uno de los mayores expertos del mundo de blockchain).



*Fuente: <https://www.blockchain.com/es/charts/my-wallet-n-users?timespan=all>*

## ■ Métodos para proteger nuestra cartera

Solo por el hecho de tener una wallet no quiere decir que ya tengamos totalmente protegidas nuestras criptomonedas y que no nos las puedan robar. Debemos, además, tener precaución y sentido común para que nuestro dinero esté a salvo.

Entre las buenas prácticas de seguridad que podemos aplicar:

- ▶ No dar a nadie nuestra clave privada. Como ya dijimos anteriormente, la clave privada sirve para firmar transacciones, es decir, si alguien la conoce podrá operar con nuestra cartera y robarnos las criptomonedas. En cuanto a esto, hay un pequeño matiz, es interesante que nadie tenga nuestra clave privada, pero que haya alguna forma de que la pueda obtener por si nos pasara algo. Imaginemos que sufrimos un accidente. Si nadie puede localizar esa clave, los fondos se perderán para siempre en lugar de pasar a nuestros herederos.
- ▶ Otra forma que tenemos de almacenar la clave privada podría ser en un papel y en una consigna que solo pudiera ser accesible si se dan unas condiciones pactadas.

Es igual de importante que nadie acceda a nuestros fondos sin nuestra autorización, como que puedan acceder si nos pasa algo a nosotros.

En caso de que pensemos que no hemos sido cuidadosos y creamos que alguien se ha podido hacer con la clave privada de nuestra wallet, es importante crear una dirección nueva y transferir los fondos a esa dirección. Y hacerlo de forma rápida.

Si tenemos la clave privada en algún archivo guardada, es importante cifrar este

archivo y ponerle una contraseña que sea segura. Si el archivo está sin cifrar o la contraseña no es segura, el riesgo de que alguien entre en nuestro ordenador y pueda copiar el archivo es elevado.

Como es lógico, si el ordenador que estamos utilizando tiene algún tipo de malware, se podría dar el caso de que nos robaran la clave privada y perdiéramos los fondos. Tener un equipo informático libre de virus es importante para nuestra wallet.

Otro consejo que podemos dar es no conectarse a wallets online que desconocemos. Aunque parece obvio, es importantísimo evitar sitios webs e introducir nuestras claves si no estamos seguros al 100% de que es un sitio de confianza. Existen multitud de webs que se hacen pasar por sitios legítimos que lo único que buscan es robar el dinero a la gente despistada que usa su plataforma pensando que es otra.

Es importante recordar que otro gran problema al que nos podemos enfrentar es a la pérdida u olvido de las claves privadas. No hay nada peor que tener dinero en un monedero de criptomonedas y perder el acceso a este. Pues esto es bastante habitual. Tengamos cuidado.

Desde el comienzo de Bitcoin han sido muchas las personas que han perdido el acceso a todo el dinero que tenían en criptomonedas por culpa de perder las claves de acceso o por no disponer de una copia de seguridad de las wallets. Así que repetimos que es importantísimo ser cuidadosos y tener siempre una copia de seguridad de nuestras claves o de nuestros monederos.

Un ejemplo claro de pérdida millonaria en Bitcoins fue el del galés James Howells<sup>[48]</sup>.

James Howells empezó con el mundo del Bitcoin cuando la tecnología era muy incipiente y consiguió tener más de 7.000 bitcoins en su poder, desafortunadamente un día mientras hacía limpieza tiró el disco duro que contenía las claves para poder acceder a su cartera.

Pasado un tiempo, Howells se dio cuenta del error que había cometido, pero ya era demasiado tarde para poder recuperar el disco duro con los bitcoins.

Para que nos hagamos una idea de la magnitud del error que tuvo James Howells, su cartera llegó a tener un valor de más 140 millones de dólares.

Por lo tanto, recomendamos tener una copia de seguridad del wallet que estamos usando (en caso de que sea posible), o por lo menos tener una copia encriptada con una contraseña muy segura con todas las claves que tenemos.

Una idea interesante para almacenar nuestra información sensible es guardarla en un pendrive (encriptado) que a su vez guardaremos en un lugar seguro.

Algunos monederos, como hemos visto antes, disponen de un sistema de recuperación que se llama semilla o *seed*, mediante el cual podemos recuperar nuestra cartera en caso de que se nos haya olvidado el acceso mediante la introducción de diferentes palabras aleatorias que guardamos con anterioridad. Estas palabras nos serán mostradas en el momento de crear la cartera, y nunca más las volveremos a ver, así que tenemos que apuntarlas y guardarlas en un lugar seguro. Si el día de mañana perdiéramos el acceso a nuestra cartera, mediante estas palabras podremos restaurar la cartera con sus fondos intactos.

Al igual que la clave privada, quien tenga estas palabras tiene acceso a nuestra cartera. Así que hay que guardarlas con mucho cuidado.

## ■ Robo de wallets mediante phishing

Un ejemplo de phishing habitual. Recibimos un correo de un exchange en el que solemos operar con frecuencia. El correo menciona que la seguridad de nuestra cuenta ha sido comprometida, y que por nuestro bien entremos a la web mediante el siguiente enlace y cambiemos la contraseña. Vemos lo fácil que es caer en este engaño, ¿verdad?

Podemos dar un par de consejos acerca de cómo actuar en este caso. Lo primero es chequear la dirección del remitente. Normalmente con esto se detecta el engaño fácilmente, ya que no suelen proceder de un servidor ni siquiera parecido a la identidad que intentan suplantar (por ejemplo, recibir un correo de Binance desde una dirección @extra.nz).

Lo segundo es que, ante la duda de la veracidad del mail, entremos directamente en la página web desde nuestro buscador, y no haciendo click en el enlace. Una vez dentro podemos cambiar la contraseña si lo consideramos adecuado, y también sería recomendable ponerse en contacto con los servicios de atención al cliente notificándoles acerca del mail recibido.

Aunque los ataques a individuos no son tan comunes, siempre tenemos que tomar todas las precauciones posibles. Si somos descuidados puede que tengamos el ordenador infectado y que tengan nuestras claves, y que esperen a robarnos cuando tengamos muchas criptomonedas acumuladas.

La razón por la que las carteras individuales no suelen ser atacadas mediante fuerza bruta (es decir, probando millones de combinaciones alfanuméricas para ver si alguna resulta ser la clave privada) es que en el mundo de la criptografía hay una asimetría a favor del defensor. El atacante tiene que destinar una

cantidad ingente de recursos para romper la clave de su víctima. Estamos hablando de que para robar una contraseña de Bitcoin por fuerza bruta, un individuo podría estar siendo atacado por miles de ordenadores a la vez y que aun así su cartera permanezca segura.

Por eso los ataques se producen por ingeniería social. Se busca que el individuo caiga en alguna trampa y ejecute un programa malicioso. Por eso siempre se dice que el punto más débil de la seguridad es la persona. Somos muy fáciles de engañar. Seamos conscientes de ello y tomemos todas las medidas de precaución necesarias.

## **Conclusión**

Este capítulo nos ha permitido conocer cuáles son, a día de hoy, los proyectos más conocidos del ecosistema. Además, el lector se lleva unas pequeñas pinceladas de cómo pueden ser los modelos económicos de las criptomonedas, información acerca de las ICO, y cómo funcionan las carteras.

Cada uno de los apartados se podría merecer un libro por sí mismo. Todos tienen la complejidad suficiente para desarrollarlos con mucho más detalle. Pero pensamos que lo importante es enseñarle al lector el cuadro entero, y cómo están relacionadas las partes entre sí, y que profundice en aquellas áreas que más le han cautivado.

Por último, no podemos incidir más en el aspecto de la seguridad. Queremos que el lector sea consciente de que no estamos en el sistema financiero tradicional. Si

tenemos un problema con nuestra cartera o nuestras criptomonedas, nadie podrá ayudarnos. Somos los únicos responsables de nuestros activos.

## 5. Trading básico

En este capítulo vamos a tratar un tema del que todos hemos oído hablar en mayor o menor grado, ese tema es el trading.

Para los que no conozcan qué es el trading, se basa en comprar y vender activos en mercados financieros. Como habréis podido comprobar a lo largo del libro, somos unos entusiastas de las criptomonedas y, por tanto, os hablaremos más en profundidad del trading de este tipo de activos.

A todos nos suenan las diferentes historias de gente que se ha hecho millonaria gracias al trading o, como podíamos ver en la película de *El lobo de Wall Street*, donde se asociaba el trading con el emprendedor aventurero de Martin Scorsese, cuya vida es una fiesta continua en la que su mayor problema es evadir a la justicia y contar el dinero que ha ganado.

Como podéis imaginar, la realidad y la ficción no siempre van de la mano. Un ejemplo de esto es que la mayoría de los traders abandonan esta actividad cuando no llevan ni un año ejerciéndola y pasan a creer que todo es un juego manipulado y que es imposible hacerse rico mediante el trading.

Entonces, ¿a qué se debe que el trading llame tanto la atención a la gente? Para nosotros se resumen en dos cosas: la primera es adrenalina y la segunda es la idea de hacerse millonario «sin trabajar» y poder vivir viajando y sin horarios.

La gente tiene la idea de que el trading es algo sencillo y que no hay que dedicarle mucho tiempo, y en parte es normal que piensen eso, ya que es lo que recibimos de los diferentes medios. Pero la verdad detrás del trading quizás no

sea tan bonita, ya que hay que estudiar muchas gráficas, hacer *backtesting* (probar con datos pasados si una estrategia determinada hubiera arrojado resultados positivos) para saber qué resultados hubiéramos obtenido si hubiéramos aplicado la estrategia que estamos desarrollando, estudiar competidores, etc. Como ya os imaginaréis, suena a tareas complicadas, poco glamurosas y que requieren de mucho tiempo.

Hay que tener claro desde un principio que el trading «es un juego de suma cero». ¿Qué quiere decir esto? Que para que unos ganen, otros tienen que perder. Para que alguien gane 100 dólares, una persona o varias tienen que perder esos 100 dólares. También hay que matizar que no es un juego que sume cero de verdad, ya que hay alguien que siempre gana y que no muchas veces se le tiene en cuenta y estos son los operadores de bolsa (bróker) o las casas donde se hacen el intercambio de monedas (exchanges) que, mediante sus comisiones, tienen el mejor juego de todos para siempre ganar. Cada vez que realizas una compra o una venta de un activo, ellos reciben su pequeña comisión sin haber arriesgado nada en la operación.

Mucha gente no conoce que el trading no es un juego donde partamos con las mismas oportunidades que nuestros contrincantes. Ya por 2014 se estimaba que más del 40% de las operaciones diarias en los mercados financieros estaban realizadas por robots de trading. Actualmente se cree que ese número puede llegar incluso a más del 80%, pero es extremadamente difícil de averiguar, ya que en muchas ocasiones no se puede distinguir una operación de una persona de la de un programa. Sí, has leído bien, más de un 80% de las operaciones que se realizan en bolsa son llevadas a cabo por ordenadores que operan en milésimas de segundo entrando y saliendo al mercado a una velocidad que las personas

solo podríamos soñar.

No nos parece descabellado que casi todo el trading se realice mediante robots que son capaces de tener en cuenta todas las variables de los mercados en milésimas de segundo, analizar tweets de famosos, noticias de impacto, etc. Cualquier información susceptible de afectar al mercado es procesada casi instantáneamente, y se traduce en una operación. Contra eso, una persona no puede competir.

Por tanto, imagínate al trader principiante como fuimos nosotros con su papel y su boli, con su Excel, sus cuadernos, sus gráficas, luchando contra una horda de robots preparados para ganar. Es como intentar combatir una guerra de tanques con palos y piedras.

El trader principiante desconoce la importancia que puede llegar a tener la infraestructura con la que operamos. Si estamos analizando variables y observamos un patrón que me indica que un activo va a subir inmediatamente, lo más probable es que cuando quiera hacer click para abrir una posición ya se haya producido la subida. Los bancos y empresas privadas se gastan cientos de miles de euros en potentes infraestructuras para situarse lo más cerca posible de Wall Street, para intentar arañar milisegundos de rapidez, y es que para ganar las mejores posiciones todo el tiempo cuenta.

Pero bueno, no nos desanimemos, porque aun así podemos crear estrategias de trading que sean buenas a futuro, aunque te advertimos desde ahora que no va a ser algo ni fácil ni rápido, hay mucho estudio detrás de una estrategia rentable de trading y también hay que saber que la misma estrategia no te durará de por vida, en el mejor de los casos te podrá durar meses, o años, aunque lo normal son días

o semanas.

Quizás las diferencias entre el trading tradicional y el trading con criptomonedas sean pocas, pero como te dijimos anteriormente, preferimos el trading con criptomonedas porque pensamos que es un mercado menos saturado en el que la competencia está más igualada, ya que no hay tantos robots y, además, en el que nosotros desde casa podemos llegar a crear nuestros robots de trading competentes sin complejas ni caras infraestructuras.

Una de las ventajas de operar mediante robots de trading es que en un mercado como el de las criptomonedas, que está abierto 24 horas al día, los 7 días de la semana, los 365 días del año, nos podemos despreocupar y no estar pendiente todo el rato de la pantalla del ordenador, ya que nuestro robot operará siguiendo las órdenes que le hayamos programado y hará lo que haríamos nosotros si estuviéramos delante de la pantalla.

Si te ha parecido interesante todo lo que acabamos de ver, te animamos a que continúes leyendo este capítulo, donde veremos diferentes conceptos del trading, trading algorítmico y la gestión del riesgo.

## **5.1. Tipos de Análisis**

### ***5.1.1. Análisis fundamental***

El análisis fundamental de una criptomoneda o de cualquier activo o empresa es la evaluación económica y financiera junto a otras variables de la misma para

determinar su valor real, intrínseco o fundamental. En un mercado tradicional como la bolsa, se espera que todos los activos coticen a sus valores fundamentales y que, a pesar de las desviaciones que se produzcan por el camino, terminen en ese valor. Este tipo de análisis es usado para tomar decisiones de compra cuando el valor de mercado se encuentra por debajo de su valor fundamental y tomar decisiones de venta cuando se encuentre por encima.

En el caso de la bolsa tradicional, para el análisis fundamental se usan variables tales como los beneficios de una empresa, la calidad de gestión, la situación económica del país, etc. En el caso de las criptomonedas, esto se vuelve más complicado ya que Bitcoin no devuelve beneficios a fin de año ni existe un organismo que lo gestione. Por ello se han creado nuevas métricas que permitan aproximar el valor fundamental de una criptomoneda. Ejemplos de estas nuevas métricas son:

- ▶ ¿Cómo de extendido está el uso de la criptomoneda?
- ▶ ¿Qué comisiones se pagan por transacción?
- ▶ ¿Cuánto se tarda en producir una transacción?
- ▶ ¿Cuántas transacciones se producen al día?

Como vemos, no son preguntas sencillas y algunas se encuentran libres de interpretación, lo que añade una doble complejidad.

Dos de los conceptos básicos que se usan en el análisis fundamental son la oferta y demanda. Como ya sabemos, el número total de bitcoins no cambia y, al igual que el oro, cada vez se hace más difícil su extracción. Con 17 millones de bitcoins minados en 2018, cada vez se generarán nuevos bitcoins a un ritmo más

lento. Este es uno de los argumentos usados por la gente que considera que el precio del bitcoin seguirá subiendo en los próximos años. A diferencia de la moneda fiat, cuyo suministro es infinito (depende de bancos centrales y gobiernos), no podemos crear los bitcoins que queramos, por lo que evitamos el problema de crear inflación imprimiendo dinero. Y es que si nos fijamos en situaciones como la de Venezuela, donde la inflación se disparó a 8.900% en marzo de 2018, el Bitcoin se presenta como una alternativa muy atractiva contra este fenómeno, hecho que aumentaría el valor fundamental de la criptomoneda.

Además, un estudio de Chainanalysis<sup>[49]</sup> a finales de 2017 estimaba que casi cuatro millones de bitcoins habían desaparecido debido a gente que había perdido sus contraseñas. En esa cifra se incluyen los 1,1 millones de bitcoins que Satoshi Nakamoto minó en sus orígenes y que no se han movido desde entonces. Por tanto, con menos moneda en circulación, el resto valdría más.

Otro de los aspectos cruciales del análisis fundamental son los eventos que se producen en el mundo del Bitcoin. Y es que un trader de criptomonedas no puede ser ajeno a las noticias que se están produciendo en cada momento. Si miramos atrás en el tiempo, a finales de 2013 Bitcoin se posicionaba por encima de los 1.000 dólares alcanzando un pico de 1.147 dólares el 4 de diciembre; apenas dos semanas más tarde, el 18 de diciembre, el precio llegó a 522,23 dólares, lo que supone una caída de más del 50%. Lo que ocurrió fue simple, uno de los exchanges más importantes en aquella época, BTC China, dejó de aceptar depósitos en yuanes, lo que provocó un cierre al flujo de entrada de dinero.

Estos y otros eventos que veremos más adelante provocan fluctuaciones de vértigo en los precios de las criptomonedas. Por ello resulta tan importante

anticiparse a los mismos conociendo de primera mano lo que está sucediendo en el mundo. Nuestras recomendaciones más importantes se encuentran en inglés y son Reddit y Bitcointalk, donde se discuten diariamente en comunidad todos los eventos relacionados con las criptomonedas.

### ***5.1.2. Análisis técnico***

A diferencia del análisis fundamental, el análisis técnico se centra en predecir los movimientos del precio de un activo a través del estudio de los cambios de precio pasados haciendo uso de herramientas tales como figuras, indicadores o patrones. Las dos variables principales son el precio y el volumen.

Dentro de las criptomonedas, el análisis técnico es más criticado incluso que en la bolsa tradicional porque se acusa al mercado de las criptomonedas de ser un mercado manipulado, ya que pocos jugadores poseen la mayoría de bitcoins, por lo que podrían comprar o vender a su antojo para manipular el precio. Nosotros consideramos que al estar cada vez más extendido su uso, esta manipulación, en caso de que exista, terminará por desaparecer. O tendrá las mismas características que la manipulación en mercados tradicionales.

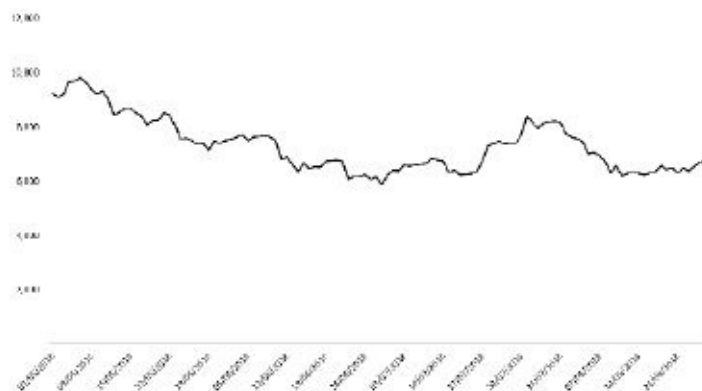
El análisis técnico tiene cientos de miles de seguidores y lo podemos observar en páginas tan conocidas como Tradingview. Esta web es una red donde los traders analizan el mercado, intercambian ideas y publican sus predicciones. Los resultados obtenidos son registrados y podemos observar la ratio de acierto de cada uno y emular sus acciones si así lo consideramos oportuno. Observamos que hay ciertos jugadores que despuntan respecto a la media, por lo que

consideramos que la mejor manera de aprender es seguir con frecuencia a estos traders y estudiar sus análisis. Nosotros en este libro proporcionamos las herramientas básicas para entender estos análisis y empezar a construir los nuestros propios.

La herramienta principal para empezar con el análisis técnico son los gráficos de precio. Existen varios tipos y os presentamos los más utilizados:

### ■ Gráfico de línea

En un gráfico de línea simplemente se representa el precio del activo al final de cada periodo. Si, por ejemplo, vemos un gráfico de línea diario, cada punto simboliza el precio al final de ese día. Podemos ver un ejemplo sencillo en la gráfica de abajo:



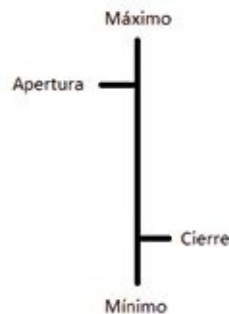
### ■ Gráfico de barras

Aunque un gráfico de línea puede enseñarnos tendencias de manera más visual, omitimos información crucial. Imaginemos que ayer cerramos a un precio de 6.100 € y durante el transcurso de hoy llegamos a un pico de 7.000 € y a un

fondo de 5.200 €. Al final del día cerramos con un precio de 6.150 €. En ningún gráfico de línea seríamos capaces de ver estas fluctuaciones y se podría llegar a pensar que el precio ha sido estable pero la realidad es que ha habido una volatilidad muy alta.

En el capítulo siguiente de las velas japonesas os explicaremos cómo sacar toda la información de este tipo de gráficos, y entenderemos qué es la apertura, cierre, mínimo y máximo.

Un ejemplo de una barra del gráfico de barras es la imagen que tenemos a continuación, en donde encontraríamos cuatro valores, con la información de apertura y cierre de la barra y además con el máximo y mínimo valor al que se llegó en esa ventana temporal.



## ■ Velas japonesas

Los gráficos de velas japonesas son similares a los gráficos de barra y son una herramienta muy útil sobre la que se apoyan la mayoría de traders, y por eso mismo están presentes en todas las plataformas financieras. Aunque al principio puedan parecer simplemente barras de diferentes longitudes, guardan muchísima información que os explicaremos a continuación.

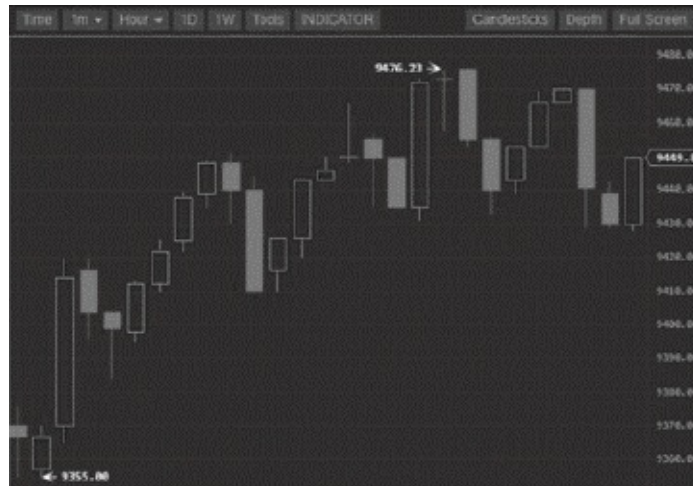
Es muy importante saber interpretar los gráficos de velas para poder extraer toda la información e intentar anticiparnos al movimiento de precio que sucederá a continuación. Muchas veces esto es complicado, pero si sabemos leer la información que nos están ofreciendo entenderemos mejor lo que pasa en el mercado.

Hay que recordar que intentar anticiparse al cambio de precio de un activo no es una ciencia exacta y no siempre acertaremos, porque, como ya sabemos, se trata de un juego probabilístico y en él entran muchos factores que pueden alterar nuestra predicción. De todas formas, las velas japonesas unidas a otras herramientas nos pueden servir para armar una buena estrategia de trading.

Para la explicación de las velas japonesas vamos a utilizar el mundo de las criptomonedas, que es el que más nos gusta y el que mejor conocemos.

## ■ Empezando con las velas japonesas

En la imagen siguiente podemos ver un gráfico de velas sobre el par Bitcoin/Tether (BTC/USDT) a día 25 de abril del 2018 en el exchange Binance.



Como se puede apreciar en la imagen, el precio más bajo que tenemos en el espectro de tiempo de la imagen son 9.355 USDT por Bitcoin y el más alto son 9.476 USDT por bitcoin. Las diferentes velas que encontramos nos dan información de la evolución del precio. En el caso de la imagen tenemos puesta la escala de tiempo de 1m (un minuto), pero también es interesante cambiar esta escala de tiempo para ver la evolución del precio en una escala de tiempo mayor. Tenemos la posibilidad de poner escalas de tiempo de 1m, 5m, 15m, 30m, 1h, 2h, 4h, 6h, 12h, 1D, 1W, donde la m significa minuto, la h significa hora, la D significa día y la W significa semana.



Una forma para poder ver si de verdad tiene tendencia alcista consistente es utilizar otra escala de tiempo un poco mayor para ver si nos sigue indicando que el precio va al alza. Así que vamos a utilizar la gráfica de intervalo de tiempo 12 horas para ver qué información obtenemos.



Aunque los indicadores apunten a que la tendencia sea alcista (o bajista), recuerda que esta puede cambiar bruscamente y que tenemos que protegernos para que estos cambios no nos afecten gravemente.

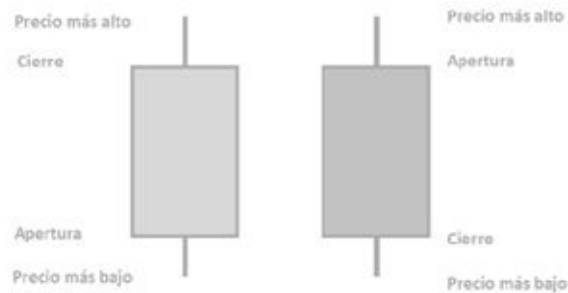
## ■ ¿Qué es eso de OHLC?

Las siglas de OHLC son Open, High, Low y Close, y como veremos a continuación son los cuatro precios que podemos obtener como información de una vela. De todas las velas siempre podemos obtener el precio de apertura y cierre de sesión, así como el precio mínimo y máximo que se ha llegado a tener en la sesión. Es importante destacar que algunas veces el precio mínimo o máximo coincide con el precio de apertura o cierre de la sesión, es decir, si hemos abierto a 9.000 € y el precio en la sesión solo ha bajado, el precio máximo de la sesión será igual al precio de apertura, ya que en ningún momento se ha sobrepasado ese precio.

Esto puede que ahora no lo tengas muy claro, pero cuando termines de leer el capítulo te parecerá facilísimo.

Para estudiar la información que nos ofrece una vela, lo primero que tenemos que tener en cuenta es que el color de la vela nos indica si la apertura ha sido a un precio mayor o menor que el cierre, hay que tener en cuenta que esto está ligado directamente al origen de tiempos, es decir, si desplazáramos el origen de tiempos cinco segundos hacia adelante o hacia atrás todas las velas de nuestro gráfico cambiarían y con ellas su color, ya que tendríamos otras aperturas, cierres, máximos y mínimos, tendríamos toda la información desplazada y, por tanto, los colores de las velas no tendrían por qué ser iguales.

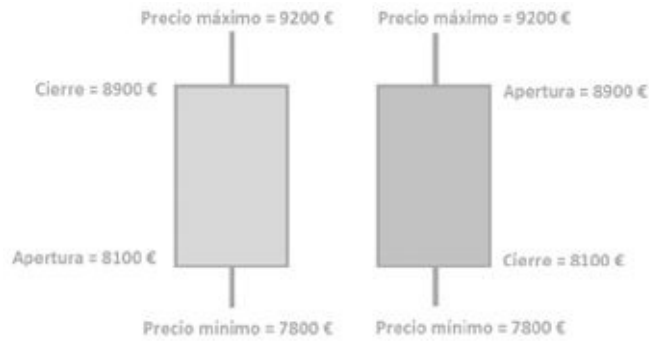
En la imagen que tenemos a continuación podemos ver que la primera vela es de color claro, esto significa que el precio con el que ha cerrado esa sesión ha sido mayor que con el que ha abierto, por tanto, ha sido alcista. En cambio, si la vela es de color oscuro significa que la sesión ha empezado con un precio más alto y se ha cerrado con un precio menor.



Ahora nos falta por saber qué son las líneas que salen hacia arriba y hacia abajo de la vela. Estas líneas nos muestran el precio que ha llegado a alcanzar el precio en esa sesión, es decir, nos muestran el precio máximo y mínimo que ha llegado a tener el activo.

Vamos con otro ejemplo para terminar de entender todo esto:

La siguiente imagen es la misma que la anterior, pero con los precios de cada una de las partes de la vela. En la figura de la izquierda podemos observar una vela de color claro que, como dijimos anteriormente, el cierre ha sido mayor a la apertura y, como podemos comprobar, efectivamente el precio del cierre (8.900 €) es mayor al precio de la apertura (8.100 €). O lo que es lo mismo, inició la sesión con un precio de 8.100 € y cuando se cerró la sesión el precio fue de 8.900 €. También podemos observar que el precio máximo en algún punto de la sesión fue de 9.200 € y que el precio mínimo fue de 7.800 €.



La vela de la derecha es de color oscuro, que como ya sabemos significa que el cierre de la sesión ha sido a un precio menor que el de la apertura. Los máximos y mínimos funcionan igual que en el ejemplo anterior.

En resumen:

Las velas japonesas son una herramienta que nos permite conocer el precio máximo y mínimo de la sesión, así como a qué precio abrió la sesión y a qué precio la cerró. Si son claras, el precio de cierre es superior al de apertura (sesión alcista) y si es oscura, el precio de cierre es menor al de apertura (sesión bajista).

## ■ Volumen

Anteriormente hemos hablado de que en el análisis técnico los dos elementos más importantes son el precio y el volumen, pero hasta ahora solo hemos visto gráficos del precio. Es hora de indagar en el volumen, y cuando nos referimos a volumen estamos haciendo referencia a la cantidad de activos (en nuestro caso, criptomonedas) que se han comprado o vendido en una ventana temporal concreta, por ejemplo, en 1 minuto, 5 minutos, 1 hora, o 1 día.

Normalmente se representan debajo del gráfico de velas mediante un gráfico de barras, como podemos observar en la figura de abajo, en el rectángulo remarcado

de la interfaz gráfica del exchange de Binance. Todas las gráficas que veremos a continuación han sido extraídas de su plataforma, accesible en <https://www.binance.com/en>.

El gráfico que tenemos en la imagen pertenece al par de Bitcoin/Tether (BTC/USDT) con la ventana temporal de un día. Las diferentes barras claras y oscuras nos indican el volumen de bitcoins que se han intercambiado en esa ventana temporal, es decir, cuántos bitcoins se han comprado y vendido cada día. Podemos observar que, al igual que las velas japonesas, tienen el mismo color en función de si el precio de cierre de ese día ha sido superior al precio de apertura o si, por el contrario, el precio de apertura ha sido superior al precio de cierre. Además, si nos fijamos en el día 17 de mayo a la hora en que se tomó la captura se llevaban intercambiados 25.439 bitcoins.



Ahora que ya entendemos qué es el volumen de operaciones, ¿por qué es importante?

Es importante porque, aunque a primera vista pueda parecer una métrica insignificante, el volumen es usado por los analistas técnicos para confirmar

tendencias o patrones.

Imaginemos que vemos una subida de un 10% en pocas horas en una criptomoneda y que para este cambio de subida tenemos dos escenarios: en el escenario A, cada vez tenemos un volumen mayor, lo que quiere decir que cada vez tenemos más compras y ventas de esa criptomoneda; en el escenario B, tenemos la cara opuesta, cada vez un volumen menor, o lo que es igual a que cada vez se compran y venden menos criptomonedas.

Del escenario A podríamos sacar una primera conclusión de que la gente sigue muy interesada en esa criptomoneda y que es más probable que el precio siga subiendo, mientras que del escenario B podríamos pensar que cada vez hay menos gente dispuesta a comprar a valores tan elevados y que podría ser indicativo de que un cambio de tendencia se aproxima. Con este simple ejemplo hemos podido comprobar lo importante que es el volumen para ayudarnos en nuestras predicciones sobre el precio en el futuro, y sobre los posibles cambios de tendencia que pueda experimentar el activo, por lo tanto, debemos tener siempre muy en cuenta tanto el precio como el volumen de transacciones que estén ocurriendo.

## ■ Bid y Ask

Entender qué es el Bid y el Ask es de las cosas más importantes en trading.

El Bid y el Ask son los precios a los que podemos comprar y vender un activo (en nuestro caso, criptomonedas). La diferencia entre ellos es comúnmente llamada horquilla o *spread* y, a continuación, os lo explicaremos de una forma muy intuitiva.

Para explicaros todos estos conceptos nos vamos a apoyar en la sencilla interfaz del exchange de Binance; es importante remarcar que los conceptos que explicaremos a continuación son válidos para todos los exchanges.



El Bid es el precio máximo al que alguien quiere comprarnos una cantidad de criptomonedas y el Ask es el precio mínimo que alguien está dispuesto a aceptar para vender una cantidad de criptomonedas.

Supongamos que queremos comprar una criptomoneda de forma directa, para ello nos interesa buscar el precio más bajo por el cual la podamos conseguir (este precio se llama Ask). Si, en cambio, lo que queremos nosotros es vender una criptomoneda nos interesará venderla al precio más alto que podamos conseguir (este precio se llama Bid).

Para encontrar el Bid y el Ask en la imagen anterior nos tenemos que fijar en el rectángulo de la izquierda. Esta imagen es la que os mostramos a continuación.

| Order Book  |                |             |
|-------------|----------------|-------------|
| Price (BTC) | Quantity (ICX) | Total (BTC) |
| 0.000429    | 339.86         | 0.14832816  |
| 0.000428    | 14.89          | 0.00606403  |
| 0.000427    | 5,367.89       | 2.21532620  |
| 0.000426    | 1,069.95       | 0.44146137  |
| 0.000425    | 41.00          | 0.01691250  |
| 0.000420    | 1,800.00       | 0.74160000  |
| 0.000419    | 593.40         | 0.24442146  |
| 0.000418    | 953.00         | 0.39277494  |
| 0.000415    | 845.70         | 0.34635855  |
| 0.000410    | 1,087.27       | 0.09346797  |
| 0.000404    | 2,303.43       | 0.90995157  |
| 0.000400    | 11,743.26      | 4.81474400  |
| 0.000399    | 3,227.69       | 1.32303913  |
| 0.000398    | 2,226.32       | 0.91234594  |
| 0.000390    | 112.71         | 0.04516602  |
| 0.0004095   | 64.28          | 0.02632266  |
| 0.0004096 ↑ |                |             |
| 0.000406    | 47.23          | 0.01929618  |
| 0.000405    | 105.61         | 0.04314189  |
| 0.000404    | 220.00         | 0.08864800  |
| 0.000403    | 673.97         | 0.27518195  |
| 0.000400    | 1,019.54       | 0.41597232  |
| 0.000393    | 1,507.33       | 0.61303551  |
| 0.000372    | 738.56         | 0.30074976  |
| 0.000371    | 118.50         | 0.04511136  |
| 0.000370    | 154.44         | 0.06285736  |
| 0.000369    | 1,313.94       | 0.53464219  |
| 0.000367    | 49.17          | 0.01909744  |
| 0.000364    | 70.94          | 0.02603802  |
| 0.000363    | 5.20           | 0.00211276  |
| 0.000361    | 90.64          | 0.03889690  |
| 0.000360    | 528.72         | 0.21466032  |
| 0.000359    | 68.02          | 0.02700932  |

En la imagen anterior encontramos los precios a los que la gente está dispuesta a comprar (precios en la parte inferior) y a vender (precios en la parte superior) la criptomoneda y, además, encontramos en el medio el último precio al que se ha hecho el último intercambio. En nuestro caso estamos usando el par de divisas ICX/BTC.

Tenemos que tener claro que si alguien está dispuesto a vender una parte de la criptomoneda, nosotros la acción que podemos tomar para coger ese precio es la contraria, es decir, le estaremos comprando una parte de la criptomoneda.

Además de todo esto, tenemos que tener en cuenta que quizás no podamos comprar todo lo que queramos a ese precio y nos tengamos que fijar en la cantidad que alguien ha puesto a la venta.

En la imagen que tenemos a continuación podemos ver que el Ask es igual a 0,0004095 con una cantidad de 64,28 ICX, lo que representa 0,02632266 bitcoins. En caso de que quisiéramos comprar una cantidad mayor, nos tendríamos que ir al siguiente vendedor, que en este caso tendría el precio de

0,0004096 con una cantidad de 112,71 ICX (0,04616602 bitcoins). Sencillo, ¿verdad?

|           |        |            |
|-----------|--------|------------|
| 0.0004096 | 112.71 | 0.04616602 |
| 0.0004095 | 64.28  | 0.02632296 |
| 0.0004096 | 47.23  | 0.01929818 |
| 0.0004085 | 165.81 | 0.04314189 |
| 0.0004084 | 220.00 | 0.08984300 |

Para tener un ejemplo claro de Bid, lo único que deberíamos hacer es la dualidad de la operación, teniendo como Bid el precio a 0,0004086 con una cantidad de 47,23 ICX (0,01929818); al igual que nos pasaba con el Ask, en caso de que queramos vender más cantidad tendremos que usar también el siguiente precio.

En relación directa con lo que acabamos de ver tenemos las operaciones de Limit y Market, que os explicamos a continuación.

## ■ Operaciones de compra y venta a Limit y Market

Otro concepto fundamental dentro del trading son el tipo de operaciones que vamos a realizar tanto para comprar como para vender. Podemos diferenciar dos grandes tipos de operación de compra o venta, y estos tipos son las operaciones a Market y las operaciones a Limit.

The screenshot shows a trading interface with two main sections: 'Comprar ICX' (Buy ICX) and 'Vender ICX' (Sell ICX). Each section has a 'Precio' (Price) field set to 0.0004083, a 'Cantidad' (Quantity) field, and a 'Total' field. Below the quantity field are percentage buttons: 25%, 50%, 75%, and 100%. The interface also includes tabs for 'Limit', 'Market', and 'Stop-Limit' at the top, and a 'BTC Balder' label next to the 'Comprar ICX' section.

Imaginemos primero que queremos realizar una compra de 200 ICX y

seleccionamos la opción de Market. La opción Market provocará que la compra de los 200 ICX se realiza de manera instantánea independientemente del precio de compra disponible (Ask).

|           |           |            |
|-----------|-----------|------------|
| 0.0004110 | 1,687.27  | 0.69346797 |
| 0.0004104 | 2,363.43  | 0.96995167 |
| 0.0004100 | 11,743.28 | 4.81474480 |
| 0.0004099 | 3,227.69  | 1.32303013 |
| 0.0004098 | 2,226.32  | 0.91234594 |
| 0.0004096 | 112.71    | 0.04516602 |
| 0.0004095 | 64.28     | 0.02532265 |

En la imagen anterior os mostramos la tabla de los Ask (precios de compra directa) que tenemos para los ICX.

Si en el escenario de comprar a Market ejecutamos la orden, compraríamos 64,28 ICX a un precio de 0,0004095, 112,71 ICX a un precio de 0,0004096 y 23,01 ICX a un precio de 0,0004098 (los 23,01 representa la cantidad que nos falta para llegar a 200 ICX después de haber comprado 64,28 y 112,71 ICX). Como podemos ver en la imagen anterior, al utilizar la opción de Market se van utilizando (se van gastando) los mejores precios de compra uno a uno hasta llegar a la cantidad deseada por nosotros, en nuestro caso 200 ICX.

Tenemos que tener cuidado cuando queramos hacer una gran compra a Market, ya que podemos consumir un gran rango de precios y que nuestro precio medio de compra resulte más elevado que si lo hubiéramos comprado en paquetes pequeños.

En la imagen siguiente tenemos el precio de los Bid y Ask, así como el precio al que se realizó la última transacción.

|                    |        |            |
|--------------------|--------|------------|
| 0.0004096          | 112.71 | 0.04616602 |
| 0.0004095          | 64.28  | 0.02632266 |
| <b>0.0004096 ↑</b> |        | <b>ask</b> |
| 0.0004086          | 47.23  | 0.01029818 |
| 0.0004085          | 105.61 | 0.04314169 |
| 0.0004084          | 220.00 | 0.08984800 |

Si, por el contrario, imaginamos ahora que los precios de mercado nos parecen muy caros o que queremos dejar una orden puesta con la corazonada de que se puede realizar mientras dormimos porque pensamos que los precios van a bajar. Entonces lo que tenemos que hacer es una operación Limit.

Para realizar la orden a Limit, podemos poner el precio que creamos conveniente; en nuestro ejemplo pensamos que el precio del par ICX/BTC va a bajar a lo largo del día y vamos a poner una orden de compra a 0,0004010. Recordemos que el precio del Bid es 0,0004086, así que nuestro precio de compra va a ser mucho más bajo que el mejor precio de compra y, por lo tanto, nuestra orden puede que no se llegue a ejecutar nunca.

Una estrategia común si queremos comprar una criptomoneda es poner el precio del Bid más un poco. En nuestro caso podríamos poner 0,0004087, ya que es un número más grande que el Bid (0,0004086) y tendríamos un mejor precio de compra que si lo hiciéramos al Ask (0,0004095). Hemos conseguido ganar si se realiza la operación  $0,0004095 - 0,0004087 = 0,0000008$  (bitcoins) por cada ICX que compramos. La operación no tendría por qué realizarse, pero es muy probable que dependiendo del volumen de transacciones que haya sí llegue a ocurrir.

Recordamos de nuevo que una operación de Limit se puede ejecutar o no, ya que es una orden que mandamos al mercado, pero puede que nunca llegue a cruzarse. Si tenemos mala suerte alguien podría aplicar la estrategia anterior y nos podrían adelantar de la misma manera que nosotros lo hemos hecho y podría ocurrir que

el precio nunca llegara al límite que hemos puesto. Sin embargo, si conseguimos que la operación se realice, habremos conseguido comprar 200 ICX a un precio muy inferior que con la operación Market.

Suponemos que ahora te estarás preguntando qué tipo de operación es mejor. La respuesta es depende. Tenemos que ser siempre conscientes del objetivo y de nuestra forma de hacer trading. Si quieres comprar una criptomoneda para mantenerla en cartera durante meses o años, posiblemente puedas comprarla a Market, si la cantidad es pequeña respecto al volumen de esa criptomoneda. Ahora bien, si haces trading, lo más probable es que necesites utilizar las órdenes tipo Limit para que tu estrategia sea rentable.

Ahora vamos a comparar la operación de Limit y Market que hemos visto anteriormente.

La diferencia de precio entre los dos casos se puede calcular fácilmente:

Market: 64,28 ICX a un precio de 0,0004095, 112,71 ICX a un precio de 0,0004096 y 23,01 ICX a un precio de 0,0004098.

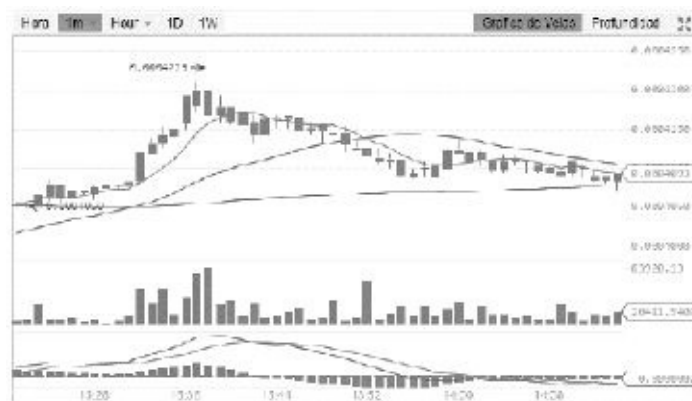
$64,28 \times 0,0004095 + 112,71 \times 0,0004096 + 23,01 \times 0,0004098 = 0,081918$  bitcoins.

Limit:  $200 \times 0,0004086 = 0,081720$  bitcoins.

La diferencia entre ambos casos es 0,000198 bitcoins, suponiendo un precio de bitcoin de 8.000 € hablamos de una diferencia de 1.584 €. Hablamos de un 0,25% aproximadamente, este porcentaje, como te dijimos anteriormente, te podrá parecer alto o bajo dependiendo de tu enfoque como trader. Si, por ejemplo, tu intención es *holdear* (mantener en cartera) una moneda, te puede

parecer insignificante, ya que suponemos que aspirarás a doblar, triplicar, hacer un x10, etc. Pero si tu idea es hacer day trading y conseguir un 1% en la operación, ese 0,25% se convierte en un gran problema.

Por otro lado, tenemos que tener en cuenta la alta volatilidad de las criptomonedas, ya que podríamos estar hablando de diferencias muy superiores o muy inferiores. Como hemos visto, la opción Market dependerá completamente del segundo en el que ejecutemos la operación. Imaginemos un escenario como la figura de abajo. Si tenemos la mala suerte de ejecutar nuestra operación de Market en el momento exacto en el que el precio está tocando máximos 0,0004229, estaríamos comprando a un porcentaje muy superior a la media de los últimos minutos.



## ■ Order book

Otro concepto clave que debemos aprender antes de comenzar a hacer trading, tanto dentro como fuera del mundo de las criptomonedas, es el historial de transacciones. De la misma interfaz que hemos visto en el apartado de Bid y Ask, si observamos abajo a la derecha podemos encontrar el historial de

transacciones, es decir, la información sobre todas las transacciones que se han producido en la plataforma en tiempo real.



Podemos ver este historial aumentado en la imagen de abajo.

| Historial de Transacciones |        |          |
|----------------------------|--------|----------|
| 0.0004096                  | 11.76  | 11:49:40 |
| 0.0004087                  | 84.28  | 11:49:38 |
| 0.0004095                  | 341.11 | 11:49:38 |
| 0.0004095                  | 10.68  | 11:49:37 |
| 0.0004096                  | 484.97 | 11:49:34 |
| 0.0004095                  | 16.25  | 11:49:34 |
| 0.0004090                  | 64.12  | 11:49:34 |
| 0.0004094                  | 25.48  | 11:49:33 |
| 0.0004094                  | 6.66   | 11:49:32 |
| 0.0004093                  | 10.97  | 11:49:32 |
| 0.0004086                  | 47.23  | 11:49:31 |
| 0.0004085                  | 453.58 | 11:49:31 |
| 0.0004089                  | 813.12 | 11:49:31 |
| 0.0004085                  | 102.00 | 11:49:30 |
| 0.0004093                  | 9.08   | 11:49:29 |
| 0.0004086                  | 9.08   | 11:49:28 |
| 0.0004093                  | 24.39  | 11:49:28 |

Lo primero que vemos en la columna de la izquierda es el valor al que se ha producido la transacción, nada complicado. El color nos indica de qué lado se ha consumido la transacción. Como hemos visto en el apartado anterior, si queremos comprar tenemos que usar uno de los Asks existentes con una operación a Market o convertirnos nosotros en uno de los Bids mediante una

operación a Limit y esperar. En cualquier caso, siempre que se produce una operación, es porque se han casado los valores del Bid y el Ask, ya que el Bid y el Ask siempre están separados. El color que vemos en el historial de transacciones simplemente nos indica si se ha consumido una compra o una venta. Cuando nos encontramos un precio de operación en color verde significa que se ha realizado una compra, por lo que al menos uno de los Asks se ha visto reducido en una cantidad. Por el contrario, una operación con un precio en color rojo indica que se ha realizado una venta.

Es importante resaltar el hecho de que, por ejemplo, encontrarnos muchas operaciones de color verde de manera seguida no tiene por qué significar que el precio está aumentando, ya que podría darse el caso de que, aunque se estuvieran realizado compras y más compras a Market, más gente estuviera dispuesta a vender a ese precio y el Ask aumentara más rápido de lo que las transacciones lo reducen.

La segunda columna nos indica la cantidad de criptomonedas con las que se ha realizado una operación. Aunque pueda parecer insignificante, este dato esconde más información de la que puede parecer en un primer momento. Imaginemos por un momento la siguiente situación:

|           |
|-----------|
| Asks:     |
| 180 10,32 |
| 167 3,1   |
| 166 7,2   |
| 165 2,1   |
| 164 0,5   |

|          |
|----------|
| Bids:    |
| 162 1,5  |
| 159 3,5  |
| 155 2,4  |
| 154 12,5 |
| 141 0,2  |

Como hemos aprendido, miramos la imagen y sabemos gracias a la lista de Asks que alguien o varias personas están dispuestos a vender 0,5 unidades a un valor de 164; 2,1 unidades a 165; 7,2 unidades a 166; 3,1 unidades a 167 y 10,32 unidades a 180. A simple vista, puede parecer un hueco muy grande entre los precios 167 y 180, pero en mercados de criptomonedas, al no existir una liquidez tan grande como en la bolsa, estas situaciones se pueden encontrar a menudo.

Ahora bien, imaginemos que soy un inversor muy potente que decide comprar 13 unidades de esta criptomoneda mediante una operación a Market porque invierto a largo plazo y no me he preocupado de mirar la lista de Asks. Lo que ocurriría, como ya hemos visto, es que consumiríamos los Asks de 164 a 167, pero además compraríamos 0,1 unidades a un precio de 180, ya que sumando las cantidades de 164 a 167 nos da un total de  $0,5 + 2,1 + 7,2 + 3,1 = 12,9$ . Al haber comprado 13 unidades, estaría comprando 0,1 unidades a un precio muy superior al que mucha gente estaba dispuesto a vender. Esto provoca que, si alguien está mirando el precio de esta criptomoneda justo después de que se realice la operación a Market pueda llegar a pensar que se encuentra el precio de manera estable en 180, mientras que la realidad es que un inversor potente ha consumido

la mayoría de los Asks.

Se pueden producir dos efectos: el primero es que la comunidad piense que esta moneda vale 180 y los nuevos valores se establezcan alrededor de esa cantidad, lo que puede acusarse de manipulaciones de precio al poder ser clasificado como un «pump», como veremos más adelante. Otro efecto posible es que alguien con operaciones a Market siga comprando a un precio de 180 y vea cómo la gente vuelve a vender en torno a los 164, precio anterior a mi operación puntual, y pierda un alto porcentaje en cuestión de segundos.

Finalmente, la tercera columna del historial de transacciones evidentemente indica la hora a la que se ha realizado la transacción.

## ■ Profundidad

Una de las principales herramientas y uno de los primeros gráficos que se enseñan en cursos de trading es el llamado gráfico de profundidad (*depth chart* en inglés).

Antes de continuar recomendamos que se tengan claros los conceptos de Bid y Ask, y de cómo forman el *Order book*.

Como recordatorio, el Order book es el libro donde se registran todos los Bid y Ask disponibles en un instante determinado, es decir, las cantidades y precios a los que la gente está dispuesta a comprar y a vender un activo. Y el gráfico de profundidad es la representación gráfica de este Order book.

Esto quiere decir que el gráfico de profundidad nos muestra de forma ordenada la oferta y demanda. Al final, el Order book es como una gran subasta donde

cada persona fija el precio que considera justo.

Pasemos a la acción y veamos de qué estamos hablando. El gráfico en concreto es del bitcoin.



Por un lado, tenemos la escalera de la izquierda que hace referencia a los Bids, los precios a los que la gente está dispuesta a comprar. Enfrente suya se encuentra la escalera que hace referencia a los Asks, los precios a los que la gente está dispuesta a vender.

Podemos encontrar el precio del Bid y el Ask en los dos recuadros pequeños que separan las dos escaleras; como se puede comprobar, los valores son de 9.260 y 9.261,53 USDT. Podemos ver que entre estos dos valores no hay nada, es el espacio que separa las escaleras. Este hueco es lo que comúnmente se conoce como *spread*. En mercados más ajustados este spread puede que sea inferior a la centésima. En otros mercados encontramos spreads mucho más grandes; por regla general, cuanto más líquido sea un mercado, menos spread tendrá.

La liquidez de un mercado está relacionada con el volumen de operaciones realizadas y con la oferta y demanda disponible. Cuanto más líquido sea el mercado más oferta y demanda habrá, menos diferencia habrá entre los Bids y

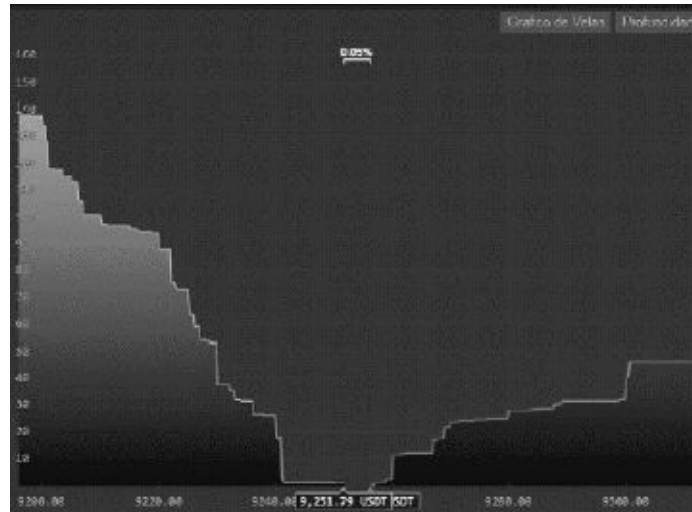
los Asks, el spread se reducirá y será posible poder comprar o vender una gran cantidad de activos sin que resulte alterado de forma significativa el valor del activo.

Volviendo a la profundidad de mercado, si empezamos por la escalera derecha (los Ask), podemos ver que el menor Ask es 9.261,53 dólares con una cantidad de 0,233017 BTC. Esta cantidad es lo que simboliza el eje vertical, la cantidad que está puesta a la venta. Es el mejor precio que podemos conseguir si queremos que nuestra operación entre de manera instantánea (operación a Market).

Si miramos el Order book vemos que el siguiente Ask es igual a 9.262,64 dólares con una cantidad de 1 BTC. Notamos que la altura de este segundo escalón es mayor que la del primero por la cantidad. Mientras que el primer Ask tenía una cantidad de 0,233017 BTC, el segundo tiene una cantidad unas cuatro veces mayor. La escalera de Bids se estudia de manera similar.

Una vez tenemos claro cómo se representa este gráfico, ¿cómo me sirve a mí para tomar decisiones?

El gráfico presentado antes es una pequeña porción de todo el gráfico de profundidad, hemos hecho zoom para poder explicar cómo se construye. Para poder sacar todo el potencial necesitamos estudiarlo desde más atrás, como vemos en la siguiente imagen:



Ahora no podemos ver con detalle los diferentes escalones, pero tenemos una imagen mucho más importante: estamos viendo cómo hay una mayor oferta que demanda en el intervalo de 9.200 a 9.300 USDT.

En un escenario ideal, esta presión que ejerce toda la gente que quiere comprar empujaría el precio al alza hasta que se equilibrasen oferta y demanda. Sin embargo, el estudio de la profundidad no es una ciencia exacta y encontraremos momentos como el que vemos en la gráfica en los que hay mucha gente queriendo comprar y, sin motivo aparente, el precio empieza a bajar mientras desaparece esa demanda.

Por lo tanto, no recomendamos el estudio aislado de esta métrica, pero sí recomendamos tomarla como apoyo para complementar nuestros análisis y poder desarrollar una estrategia de trading más sólida.

## ■ Tendencia

Una tendencia no es más que la dirección general hacia la que se está moviendo el precio de un activo; como vimos muy brevemente en el capítulo de las velas,

nos ayudan para saber en qué dirección va el precio.

Podemos encontrar tres tipos diferenciados de tendencias:

- Tendencia alcista: En este tipo de tendencia observamos una serie de picos o máximos cada vez mayores y una serie de valles o mínimos también cada vez más altos, como podemos ver en la figura.



- Tendencia bajista: Al contrario que en la tendencia alcista, observamos máximos y mínimos cada vez menores, como vemos en la figura.



- Tendencia lateral o ausencia de tendencia: Este caso podría definirse de manera sencilla como la ausencia de cualquiera de las dos tendencias vistas previamente. Este tipo de tendencia nos indica un equilibrio en el precio. Vemos un ejemplo en la siguiente imagen.



Lógicamente, esta tendencia dependerá del horizonte temporal que escojamos. Puede que mirando una gráfica horaria veamos una tendencia alcista mientras que si escogemos una gráfica mensual veamos un claro descenso en el precio.

Por ello se distinguen normalmente tres tipos de tendencias: de corto, medio y largo plazo. En el gráfico de abajo sacado de Tradingview podemos ver una tendencia alcista de corto plazo a finales de junio, una tendencia bajista desde mediados de junio hasta septiembre y una tendencia alcista a lo largo del segundo semestre de 2017.



Es importante mencionar que, dentro del análisis técnico, cuando identificamos una tendencia alcista, la línea que une los mínimos se considera una línea de soporte. Esta línea de soporte nos indicaría una línea por debajo de la cual el precio no debería de caer, y en caso de que esto sucediese, nos haría pensar que se ha producido un cambio de tendencia.

De la misma manera, cuando se identifica una tendencia bajista, la línea que une los máximos representa una línea de soporte que se puede utilizar para poner

nuestras órdenes de venta. Para ilustrar este caso observemos un ejemplo concreto dentro de Binance:



Tras haber identificado una línea de soporte uniendo los máximos de los precios, podemos ver cómo claramente en el círculo se rompe esta línea de soporte. En ese momento es cuando debemos estar atentos porque se nos ha indicado un posible cambio de tendencia. Mirando el resto de la gráfica comprobamos este cambio y cómo pasamos de una tendencia bajista a una tendencia alcista.

Por supuesto, este ejemplo no se cumple el 100% de las veces, ya que si no todo sería un camino de rosas. Está en manos del trader dibujar las líneas correctas de tendencia, estudiar el volumen asociado, analizar los indicadores que veremos más adelante, observar si se ha producido una falsa rotura y demás estrategias que hacen al trader un experto en la materia.

## ■ Soportes y resistencias

En el apartado anterior hemos mencionado cómo en tendencias alcistas se producen líneas de soporte, y en las tendencias bajistas, líneas de resistencia. Pero este tipo de líneas no se limitan a situaciones en las que encontramos una tendencia bien definida. Aun cuando no haya una tendencia clara o nos

encontremos en una tendencia lateral, podemos aprovecharnos de estas líneas para obtener un beneficio.

Una resistencia es una zona donde la oferta es mayor que la demanda y, por lo tanto, las compras no pueden absorber todas las opciones de venta que se efectúan, por lo que cada vez la gente está dispuesta a vender más barato, porque consideran que el precio no va a aumentar más y, por lo tanto, se entra en una bajada del precio. Podemos observar un claro ejemplo de resistencia en la figura siguiente.



La segunda línea nos enseña cómo el precio de la criptomoneda se acerca dos veces seguidas a 120 y no consigue superarlo. Y es que al acercarse por segunda vez a una resistencia que no consiguió superar momentos antes, la esperanza del mercado en que la supere es menor, por lo que la gente vende sus activos esperando una bajada como es el caso.

De manera análoga, un soporte es una zona donde la demanda es mayor que la oferta y por lo tanto el precio suele rebotar hacia arriba en estas ocasiones. Observamos un ejemplo en la siguiente figura.



En dos intentos el precio se acerca a 0,075950 y después de la segunda la tendencia cambió para acercarse a una resistencia de 0,081628.

Cuantas más veces se acerque el precio a un soporte o a una resistencia, menos esperanza se tiene en que esa barrera se pueda romper. También es importante el tiempo en el que se ha mantenido esa barrera, así como el volumen que se produce en una resistencia. A mayor volumen, mayor significativa será dicha barrera.

Un fenómeno común que observaremos cuando se rompa una de estas barreras es la transformación de un soporte en una resistencia y viceversa. En la siguiente figura podemos ver cómo una resistencia, una vez que se rompe, se convierte en soporte.



## ■ Indicadores básicos

Dentro del análisis técnico los indicadores son métricas estadísticas que nos

ayudan a estimar cambios en las tendencias de precio o identificar patrones en el movimiento del mismo. Dentro de los indicadores debemos hacer una primera distinción de los mismos entre:

- ▶ Indicadores adelantados o *Leading Indicators*: Estos indicadores intentan predecir el cambio de tendencia en el precio de un activo. De los más conocidos y usados son el RSI y el oscilador estocástico.
- ▶ Indicadores retardados o *Lagging indicators*: Estos indicadores nos advierten de un cambio en la tendencia una vez que ya se haya producido. Uno de los indicadores más conocidos es la media móvil.

Además, para los indicadores es necesaria una segunda distinción: indicadores de tendencia e indicadores de momento. A continuación, los veremos con más detalle.

## ■ Indicadores de tendencia

Estos indicadores miden la dirección y la fuerza con la que se está produciendo uno de los tipos de tendencia que hemos visto anteriormente. Los dos indicadores de tendencia que vamos a ver son las medias móviles simples y exponenciales. Ambos indicadores son retardados.

## ■ Media móvil

Una media móvil es un indicador que ayuda a filtrar el ruido debido a la volatilidad del precio de un activo. Hay diversos tipos y vamos a ver las dos medias más usadas:

- Media móvil simple (SMA): Existen infinitas medias móviles simples, tantas como días queramos elegir. Para ilustrar esta media ponemos un ejemplo de una media móvil simple de cinco días:

| Día    | Precio de cierre | Media móvil simple (5 días) |
|--------|------------------|-----------------------------|
| 12-Jun | 14               |                             |
| 13-Jun | 15               |                             |
| 14-Jun | 16               |                             |
| 15-Jun | 17               |                             |
| 16-Jun | 18               | 16                          |
| 17-Jun | 16               | 16.4                        |
| 18-Jun | 15               | 16.4                        |
| 19-Jun | 15               | 16.2                        |

Así, la media móvil simple el 16 de junio será la suma de los precios de cierre de los últimos cinco días dividido entre 5. En este caso  $(14 + 15 + 16 + 17 + 18) / 5 = 16$ . De la misma manera se calculan el resto de datos.

Ahora que sabemos calcularla vamos a ver cómo tomar decisiones. Para ello miraremos la segunda línea de la figura de abajo. Es la media móvil de los últimos siete días y nos la proporciona Binance en sus gráficos:



Cuando el precio se encuentra por encima de la media móvil nos encontramos en una tendencia alcista, mientras que si se encuentra por debajo nos encontramos en una tendencia bajista. En una tendencia alcista, la media móvil sirve de soporte; cuando el precio se está acercando a esta línea, podemos esperar que sea un buen momento para poner órdenes de compra. Así ocurre en la primera mitad

del ejemplo visto.

En la segunda mitad, al encontrarse el precio por debajo de la media móvil, esta línea sirve como resistencia y cuando el precio se acerque a la línea será buen momento para poner órdenes de venta.

Por supuesto, estas reglas no se cumplen siempre y siempre deberemos andar con mucho cuidado de que no se esté produciendo un cambio de tendencia al acercarse el precio a la media móvil.

Una de las desventajas de esta media móvil es que otorga la misma importancia al valor de hace cinco días y al valor de hoy, por lo que puede que haya cambios importantes que tardemos en notar. Para evitar este problema y otros, se usará el segundo tipo de media móvil, la media móvil exponencial.

### ■ Media móvil exponencial (EMA)

La principal diferencia con la media móvil simple es que la media móvil exponencial da más importancia a los datos más recientes. La fórmula es la siguiente:

$$EMA_t = EMA_{t-1} + K * (Precio_t - EMA_{t-1})$$

Siendo t el valor actual, t-1 el valor anterior y K un factor igual a:

$$K = 2 / (n+1)$$

Con n siendo el periodo elegido.

Para el cálculo de la primera EMA usamos el valor de la media móvil simple como valor anterior. Usando el mismo ejemplo del caso anterior, exponemos los

valores calculados de la media móvil exponencial:

| Día    | Precio de cierre | Media móvil exponencial<br>(5 días) |
|--------|------------------|-------------------------------------|
| 12-Jun | 14               |                                     |
| 13-Jun | 15               |                                     |
| 14-Jun | 16               |                                     |
| 15-Jun | 17               |                                     |
| 16-Jun | 18               | 16                                  |
| 17-Jun | 16               | 16                                  |
| 18-Jun | 15               | 15.7                                |
| 19-Jun | 15               | 15.4                                |

Al dar mayor importancia a los valores más recientes, la media móvil exponencial nos dará avisos más rápidos que la media móvil simple. Sin embargo, también nos dará más falsas señales. Por ello debemos tener en cuenta siempre que podamos ambas métricas.

Una de las estrategias más conocidas es aprovechar el cruce de dos medias móviles de períodos diferentes como punto de entrada. Así, cuando la media móvil de un periodo corto cruce de abajo a arriba a una media móvil de periodo largo, se toman opciones de compra y viceversa. Observamos un ejemplo en la figura de abajo.



La línea que sigue más de cerca las barras representa la media móvil de los últimos siete días, mientras que la línea del medio representa la media móvil de los últimos 25. En el primer círculo vemos cómo la línea móvil de periodo más corto cruza a la línea de mayor periodo de abajo a arriba, momento en el que

podríamos pensar en poner una orden de compra. En el segundo círculo podemos ver que ocurre justamente lo contrario, por lo que se nos indica poner una orden de venta.

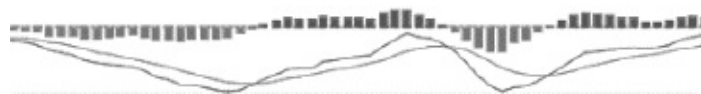
Recordamos que estos ejemplos no se cumplen siempre, por lo que debemos mirar más indicadores si queremos aumentar nuestras posibilidades de éxito.

### ■ Indicadores de momento:

Veremos tres indicadores de momento: la Media Móvil de Convergencia/Divergencia (MACD), el RSI y el Oscilador Estocástico.

### ■ MACD

Dentro del análisis técnico, el indicador MACD es uno de los indicadores más usados por traders. Para entenderlo, lo primero que necesitamos saber es que consiste en dos líneas y en un histograma, como podemos ver en la siguiente figura.



- La línea que comienza por debajo desde el comienzo es la línea principal de MACD y es la diferencia de las dos medias móviles exponenciales de 12 y 26 periodos de los precios de cierre (se resta la EMA de 26 periodos a la EMA de 12 periodos).
- La otra línea es la media móvil exponencial de la línea principal de MACD de

9 periodos y se conoce como la línea señal.

- ▶ El histograma es la diferencia entre las dos líneas que acabamos de ver.

Es importante resaltar que la mayoría de exchanges ofrecen la visualización de todos estos elementos de forma automática para nuestro análisis.

Una vez disponemos del gráfico, las dos estrategias más clásicas para tomar decisiones con el MACD son las siguientes:

- ▶ Cruces: Cuando la línea de MACD cruza de abajo a arriba a la línea señal, es un momento alcista en el que pueden tomarse opciones de compra. Al contrario, cuando la línea MACD cruza la línea señal de arriba a abajo se considera un movimiento bajista.
- ▶ La segunda estrategia consiste en observar una divergencia entre el precio y la línea de MACD. Si, por ejemplo, nos encontramos con que el precio está subiendo mientras que la línea MACD está disminuyendo, puede tratarse de un indicador de que la tendencia está a punto de cambiar.

Este indicador es muy usado en conjunto con el próximo indicador que vamos a ver.

## ■ Indicador RSI

El RSI (*Relative Strength Index* o Índice de Fuerza Relativa) es un indicador tipo oscilador que indica zonas de sobrecompra y sobreventa. Este indicador puede valer entre 0 y 100 y su fórmula es la siguiente:

$$RSI = 100 - 100 / (1 + RS)$$

Siendo  $RS = \text{ganancia media para un periodo} / \text{pérdida media para un periodo}$ .

Normalmente, el periodo elegido para calcular el RS es 14.

Como estrategia, tradicionalmente se considera que un activo está en zona de sobrecompra cuando nos encontramos valores de RSI por encima de 70. En este momento, un cambio de tendencia se hace más posible por lo que podemos encontrarnos en una buena zona de venta.

Al contrario, cuando nos encontramos un RSI con valores por debajo de 30, podemos interpretar que el activo se encuentra en zona de sobreventa y puede tratarse de un buen momento para comprar.

Algunos traders consideran que los valores de 30 y 70 pueden dar demasiadas señales falsas y ajustan estos valores a 20 y 80 o incluso a 10 y 90.

Otra estrategia común es buscar la divergencia entre el precio del activo y el valor del RSI. Como ejemplo podemos observar la figura de abajo.



La línea oscilante representa el RSI y observamos que, en el segundo círculo, aunque el precio haya alcanzado un nuevo máximo respecto al primer círculo, el valor del RSI es menor. Esta divergencia indica un potencial cambio de tendencia y, por lo tanto, un momento de venta.

### ■ Oscilador estocástico

Al igual que el RSI, el oscilador estocástico es un indicador que varía de 0 a 100 y que mide condiciones de sobrecompra y sobreventa. Está formado por dos líneas, %K y %D. Las fórmulas de ambas líneas son las siguientes:

$$\%K = 100 * (C - L14) / (H14 - L14)$$

Siendo C el precio de cierre más reciente, L14 el mínimo precio de los últimos 14 periodos y H14 el máximo precio de los últimos 14 periodos.

La segunda línea, %D, no es más que una media móvil simple de %K.

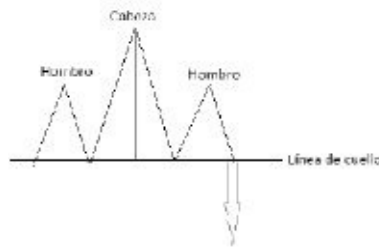
La estrategia más tradicional es elegir 20 y 80 como los umbrales de sobreventa (señal para comprar) y sobrecompra (señal para vender) respectivamente.

### ■ Chartismo

Dentro del análisis técnico, es necesario mencionar el chartismo, el cual consiste en estudiar gráficas para identificar patrones gráficos que nos ayuden a predecir el comportamiento del precio de un activo. Estos patrones pueden indicarnos un cambio de tendencia o una continuación de la misma.

Como ejemplo informativo ilustraremos el posiblemente patrón más famoso

dentro del chartismo, la figura del hombro cabeza hombro. Esta figura nos indica un posible cambio de tendencia y su nombre proviene de su semejanza a la figura de una cabeza con un hombro a cada lado, como podemos ver en la siguiente figura.



Como podemos ver, la figura de hombro cabeza hombro comienza con un primer máximo seguido de una bajada del precio hasta el precio original. A continuación, encontramos un segundo máximo superior al primero y el cual forma la cabeza. Seguimos con una segunda disminución hasta el precio original y una tercera subida al primer máximo para descender hasta el precio original formando el segundo hombro.

Esta figura nos indica que el precio puede bajar por debajo de la línea de cuello una cantidad igual a la distancia entre la misma línea de cuello y la cabeza, como indica la flecha. De todos los recursos que hemos visto para el trading, el chartismo es el que menos aconsejamos para forjar una estrategia sólida de trading. Es mucho mejor que forjemos nuestras estrategias en el precio, el volumen, la tendencia, el Order book, etcétera.

## ■ Pumps & dumps

En esta sección vamos a hablar de los pumps y dumps. Cada vez es más y más

frecuente que se hable de este tipo de operativas, y no es de extrañar, es un tema muy recurrente en el mundo de las criptomonedas y cada día gana más adeptos.

Es normal que la gente se acerque a aprender que son los pumps y los dumps con una falsa idea de hacerse millonarios en pocas operaciones, y multiplicando su dinero de forma muy rápida, ya que muchas veces se consigue doblar o triplicar la cantidad de dinero que se tiene en una inversión en tan solo minutos u horas. Pero no todo es tan bonito dentro del mundo de los pumps, la realidad que se esconde detrás de ellos es bastante inmoral y normalmente se basan en diferentes engaños o estrategias malintencionadas que buscan sacar máximo provecho a la ingenuidad de la gente.

Los pumps consisten en disparar un precio de forma artificial. Se bombea (pump) el precio poniendo de acuerdo a mucha gente para que compre a la vez un activo. Normalmente, se hace sobre criptomonedas pequeñas (para pumppear el precio del Bitcoin haría falta una cantidad de dinero astronómica). Una vez hecho esto, el precio se habrá disparado y el resto de personas, al ver lo rápido que está subiendo, quiere también meterse en la fiesta y comprar, retroalimentando la subida.

Los pumps siempre están seguidos de dumps. ¡Adivina en qué consisten!

Cuando se ha producido esta subida casi instantánea, los primeros que compraron la moneda (obviamente los promotores del pump) estarán vendiéndola para asegurar las mayores ganancias posibles. Poco a poco, el que ha ido comprando verá que cada vez el precio sube menos, hasta que finalmente comienza a caer.

¡Y comienza el pánico!

Una vez que la gente se da cuenta de que ha dejado de subir el precio del activo y empieza a bajar, todos quieren recoger sus ganancias y empiezan a vender de forma muy agitada. En la mayoría de los casos pierden mucho dinero, ya que al verse inundado el mercado por órdenes de venta y muy pocas de compra, es difícil que llegue a ejecutarse.

En este tipo de estafas no todo el mundo gana, pero siempre hay uno que sí, el que las organiza.

### ■ **Cómo se organiza un Pump & Dump**

Una persona o grupo de personas se ponen de acuerdo para bombardear durante días o semanas a través de listas de correos electrónico, grupos de Telegram, Discord, foros de internet, etc., que tal día a tal hora, en un exchange concreto, habrá un pumpeo.

A la vez que están anunciándolo, van comprando la criptomoneda que piensan pumppear, muy poco a poco para que no haya incrementos de precio o de volumen que puedan delatarles.

Llegado el día y la hora, publican qué criptomoneda se va a comprar, y comienza la carrera. La gente cree que si es extremadamente rápida puede comprar y vender antes de que comience el dump. Pero la realidad es que instantes antes de anunciar la moneda, está ya se encuentra disparada, y que posiblemente cuando ejecuten la orden de compra, ya no sean capaces de venderla más cara.

En la imagen que tenemos a continuación podemos ver uno de los textos de difusión típicos de los pumps.

1 H 10 mins TILL TAKE OFF

KEY POINTS TO REMEMBER

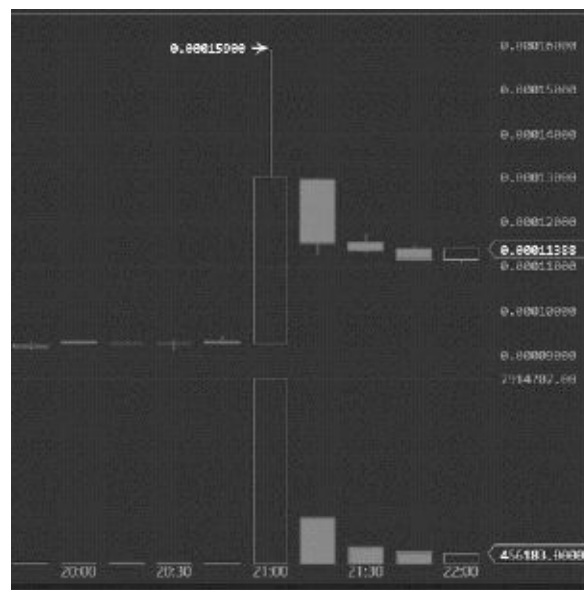
Make sure you enter your buy price at  $\times 10$  the current price. This will automatically fill at the first available price under your maximum.

BUY FAST and DON'T PANIC SELL. The longer we all hold, the higher we'll push the price.

DON'T BE GREEDY. We want everyone to do well and make money. So be sensible!

¡Fijaos que la recomendación que dan es que compres a  $\times 10$  el precio del momento del anuncio! Con eso el promotor se asegura de colocar todas las monedas que ya tenga encima y de que el precio suba de forma astronómica.

En internet es posible encontrar infinidad de grupos que se dedican a esto, muchos de ellos de pago. Estos grupos de pago se supone que te brindan la información sobre la moneda que se va a comprar unos minutos antes que al resto de personas, por lo que tendrías más «seguridad» a la hora de colocar a otro tus criptomonedas.



En la imagen anterior podemos observar un pump & dump que tuvo lugar el día 29 de abril del 2018 a las 7PM GMT en el par OAX/BTC en Binance. En la parte de arriba tenemos la evolución del precio del activo y en la de abajo la evolución del volumen negociado a las diferentes horas. Como se puede observar, el precio estaba en torno a 0,00009200 y en cuestión de minutos se puso a 0,00015900, casi el doble. Este es un claro ejemplo de pump (incremento muy rápido de precio) seguido de un dump, ya que el precio volvió a bajar rápidamente.

En la imagen anterior también podemos apreciar el gran volumen que entró a la hora del pump, y es que, como dijimos anteriormente, este tipo de estrategias necesitan a mucha gente comprando cada vez a un precio mayor para que el precio del activo suba y los organizadores puedan vender con máximos beneficios.

Desde aquí recomendamos mantenerse lejos de estas estrategias fraudulentas. Primero, porque son ilícitas, pero además porque puedes perder mucho dinero en cuestión de minutos o segundos.

Como ya dijimos anteriormente, este juego está hecho para que siempre ganen los mismos. Recuerda que el promotor del pump te está vendiendo a ti sus monedas a un precio muy superior del que las compró él.

## **5.2. Trading avanzado**

### **5.2.1. Scalping**

El *scalping* es una técnica muy conocida en el mundo del trading consistente en realizar operaciones en cortos periodos de tiempo intentando generar un beneficio pequeño. Al realizar estas operaciones en periodos cortos de tiempo se intentan realizar varias operaciones al día para que la suma de los beneficios obtenidos sea considerable.

Esta técnica es muy atractiva debido a la rapidez con la que se realizan las operaciones en el mercado. Suele realizarse mediante el apoyo de velas japonesas de 5, 10 y 15 minutos.

Podemos intentar sacar, por ejemplo, un 1% por operación de manera que si consiguiéramos realizar diez ciclos similares estaríamos hablando de un beneficio de un 10% diario.

Cobra extrema importancia el control de las pérdidas, ya que de nada nos sirve conseguir cinco ciclos de un 1% de beneficio si no pongo correctamente órdenes de stop loss y pierdo un 5% en la siguiente operación.

Aunque a priori puede parecer sencillo, hay dos barreras de entrada que aumentan la dificultad de llevar a cabo esta técnica de manera satisfactoria. La primera son las comisiones de trading y la liquidez. Para que una operación tan rápida pueda resultar rentable necesitamos un exchange con bajas comisiones y con una alta liquidez, de manera que el mercado pueda absorber nuestra orden de manera instantánea. La segunda barrera de entrada es la rapidez con la que podemos entrar al mercado.

Aunque consiga identificar de manera satisfactoria una inminente subida en el precio de un activo, puede que otros lo hayan hecho también, y puede que esos

otros sean robots que están analizando el mercado de forma continua. Por lo tanto, en el momento en el que ponga mi orden, puede que el mercado ya haya subido el precio o incluso que nos adelanten si ponemos una operación a Limit. Por este motivo siempre recomendamos trasladar a un algoritmo la estrategia que tengamos en mente y crear un robot de trading, ya que un robot siempre tomará las decisiones mucho más rápido que nosotros, y es que un pequeño porcentaje en el scalping puede resultar vital.

Al realizar scalping en el mundo de las criptomonedas también debemos tener en cuenta que se trata de un mercado continuo que no cierra. Tradicionalmente, el scalping se ha considerado más rentable en determinadas horas del mercado, por lo tanto, está en nuestra mano analizar de forma continua en qué momentos del día hay mayor movimiento de mercado para la criptomoneda que nos interese.

Como posibles estrategias se pueden aplicar aquellas que hemos visto anteriormente en el estudio del análisis técnico, así como cualquier estrategia que consideremos, no sin antes haber realizado un estudio previo para analizar las posibles ganancias que hubiéramos obtenido aplicando esa estrategia a un pasado; tan importante es definir una buena estrategia de trading como hacer un backtest de los resultados que hubiéramos obtenido con ella.

Incluso aun cuando nuestra estrategia aparezca rentable aplicándola a un pasado, no debemos pensar que hemos encontrado el santo grial, ya que en mercados de criptomonedas encontraremos momentos del día en los que la liquidez no es muy alta y, por lo tanto, nuestras propias acciones influyen en el mercado y podemos obtener resultados diferentes.

### **5.2.2. Arbitraje**

El arbitraje dentro del trading es una estrategia utilizada para intentar sacar un beneficio de la diferencia de precios entre diferentes exchanges. En un mundo perfecto todos los exchanges estarían sincronizados de manera que cualquier desviación del precio en uno de ellos tendería a volver al precio del resto de exchanges de manera instantánea. La realidad es que no ocurre eso, sino que existen diferencias que pueden llegar a ser muy elevadas.

A lo largo de los últimos años estas diferencias han ido disminuyendo. Como es lógico, cuanto más tiempo pasa más gente es consciente de esta oportunidad, por lo que empieza una competencia por ver quién consigue aprovechar esta diferencia de precios. Esta competencia es totalmente necesaria en el mercado porque disminuye las diferencias de precio entre los diferentes exchanges igualando los mercados.

Existen diferentes métodos de arbitraje, siendo los más conocidos los tres siguientes:

- **Diferencias de precio momentáneas:** Estas diferencias de precio no suelen durar más de unos minutos u horas en el mejor de los casos. Se trata de aprovechar la diferencia de precios para comprar una criptomoneda en un exchange, trasladarla a otro y venderla para sacar un beneficio. Existen herramientas web como CoinGap o incluso aplicaciones Android como CryptArbitrage que informan de manera gratuita de las oportunidades de arbitraje que encuentran.

Aunque pueda parecer sencillo hay varios factores que debemos tener en cuenta. Para empezar, debemos considerar las comisiones por comprar la criptomoneda necesaria en el primer exchange y las posibles comisiones por retirada de la misma. Igualmente, debemos considerar las comisiones por depósito en el segundo exchange, así como las posibles comisiones de la blockchain.

Adicionalmente, y de manera crítica, tenemos que tener en cuenta que la transacción de una criptomoneda entre dos exchanges no es instantánea, sino que dependiendo de la criptomoneda puede llegar a superar la hora de duración. Si en ese tiempo el precio al que esperábamos vender en el segundo exchanges baja, podemos encontrarnos con pérdidas inesperadas.

Finalmente, debemos tener en cuenta que la retirada sea posible en el primer exchanges y el depósito sea posible en el segundo. Esto último puede resultar evidente, pero a veces podemos recibir alertas de oportunidades de arbitraje en las que la retirada del primer exchanges está suspendido o vengan dadas por la suspensión temporal del trading de una criptomoneda en uno de los exchanges.

- Diferencias entre países: Esta diferencia se produce entre los exchanges que operan en distintos países. El caso más conocido se trata de la «Kimchi Premium», una diferencia en el precio del bitcoin que se produjo en los exchanges coreanos causando diferencias de hasta un 50% del precio respecto a otros exchanges fuera de Corea del Sur en diciembre de 2017. Esta diferencia llevó a CoinMarketCap a excluir los precios coreanos del cálculo del precio del bitcoin, lo que provocó una caída del mercado al no

comunicarse detalladamente.

Existen otros países en los que esta diferencia existe, pero debido a las regulaciones locales como, por ejemplo, la prohibición de algunos exchanges coreanos a los traders extranjeros, hace que sea muy difícil aprovecharse de la diferencia de precios.

- Existe una tercera oportunidad de arbitraje en el mundo de las criptomonedas y se debe a la diferencia de precios que ocurre cuando se formaliza la entrada de una criptomoneda a uno de los grandes exchanges. Una de las mayores oportunidades reside en el momento en que Binance lista una nueva criptomoneda. Binance es conocido por realizar un estudio previo de las criptomonedas muy riguroso con el objetivo de incluir únicamente proyectos serios y con potencial.

El proceso que se sigue para listar una moneda en Binance comienza por la petición del equipo de la criptomoneda vía formulario que requiere la firma de un acuerdo de confidencialidad. El resto del proceso queda oculto e incluso Binance no dispone de ningún representante para evitar posibles sobornos. De esta manera, no podemos saber cuándo se listará una moneda, ya que no se permite al equipo de la criptomoneda publicar que van a ser listados hasta el momento en que la criptomoneda está disponible para comprar y vender en la plataforma. Sin embargo, sí pueden publicar el hecho de que han rellenado el formulario y comenzado el proceso.

Cuando una criptomoneda es listada en Binance, normalmente aumenta su valor de forma muy significativa, en muchos casos de manera puntual volviendo al precio original pasadas unas horas. Al no contar con la

información de cuándo será listada una moneda, la manera de aprovechar esta subida es tener la criptomoneda en nuestra cartera, enviarla a Binance en cuanto se hace pública la información y vender a los pocos minutos. La parte complicada es analizar qué criptomonedas serán añadidas en Binance. Para ello recomendamos seguir las técnicas utilizadas en el apartado de ICO e invertir en proyectos potentes y con un buen equipo detrás.

### **5.2.3. Futuros**

Un futuro es un contrato en el que el comprador tiene la obligación de comprar una cantidad preestablecida de un activo a un precio acordado en una fecha futura especificada.

Existen dos tipos principales de uso de futuros: para evitar el riesgo que provoca la volatilidad del precio de un activo o para especular con el precio del mismo.

En el primer caso y la razón por la que los traders utilizan este tipo de contratos, es por la esperanza de obtener un beneficio. Imaginemos que tengo en mi cartera 5 bitcoins, los cuales he adquirido a un precio de 6.000 dólares el día 1 del mes y mi análisis del mercado me dice que el precio del mercado puede caer hasta los 5.000 dólares el día 30 del mismo mes. Para poder aprovecharme de esta bajada, establezco un contrato con una contraparte en el que el día 30 esté obligado a comprarme mis 5 bitcoins a un precio de 6.000 dólares. Lógicamente, la contraparte piensa que el precio del bitcoin va a subir y por ello acepta el contrato. Si llegamos al día 30 y el precio del bitcoin ha caído a 5.500 dólares, la contraparte me pagará 30.000 dólares por mis 5 bitcoins, aunque el precio del

mercado haya caído. Por el contrario, si el precio del bitcoin sube a 6.500 dólares, esa persona me seguirá comprando mis 5 bitcoins por 30.000 dólares, pero obtendría un beneficio instantáneo vendiéndolos por 32.500 dólares.

Como cada una de las partes piensa que el precio en el futuro tomará una dirección contraria, se hacen contratos donde haya obligación de comprar o vender un determinado número de activos, y de esta forma poder ganar dinero.

El segundo motivo por el cual la gente puede usar este tipo de contratos es para protegerse de la volatilidad de un activo. Imaginemos que tenemos una fábrica de cerveza y tenemos un proveedor de cebada. Si no ponemos medidas, corremos el riesgo de que nuestros beneficios aumenten o disminuyan según el precio que nos dé nuestro proveedor. Una mala temporada podría encarecer el precio de la cebada y podría provocar una reducción de nuestros beneficios, ya que no podemos encarecer el precio de la cerveza. Para evitar este riesgo, podríamos establecer un contrato futuro con una tercera parte en la que estuviéramos obligados a comprar una cantidad de cebada preestablecida al precio sobre el que hemos realizado nuestro plan de negocios, evitando los riesgos por la volatilidad del precio de la cebada. No buscamos un beneficio económico con el contrato, sino estabilizar nuestro beneficio.

Dentro del mundo de las criptomonedas, el exchange más conocido que ofrece la posibilidad de comprar futuros probablemente sea BitMex. Además de ofrecer este tipo de contratos para especular, nos permite hacerlo con un apalancamiento de x100, por lo que no es necesario disponer de todo el capital para poder operar con la cantidad que queremos. En el capítulo de gestión del riesgo veremos más en profundidad de qué se trata el apalancamiento y por qué puede ser una herramienta peligrosa de utilizar si no tenemos claro cómo funciona.

Por último, no debemos confundir este contrato con el Contrato Permanente o *Perpetual Contract* que se ofrece en la plataforma. Un *Perpetual Contract* es un producto derivado similar a un contrato de futuro, pero en el que no existe una fecha de liquidación y en el que cada ocho horas, según el sentimiento de mercado, las personas que se han posicionado en largo pagan un porcentaje a los que se han posicionado en corto o viceversa. Se trata de una fórmula aún compleja, por lo que este tipo de derivado debería ser utilizado únicamente por traders más avanzados.

#### **5.2.4. Trading algorítmico**

El trading algorítmico consiste en utilizar robots que ejecuten órdenes de compra y venta de manera automática cuando se cumplen unas condiciones en el mercado. Estos robots analizan diferentes condiciones como pueden ser el precio, o diferentes indicadores como los que hemos visto previamente para la toma de decisiones. Un robot no hará nada que no esté implementado dentro del algoritmo. No tiene capacidad de pensar. Actúa bajo un supuesto de: si sucede A, entonces B. Esto puede llegar a ser extremadamente complejo, según la estrategia que tengamos diseñada.

Existen técnicas de Machine Learning (una rama de la inteligencia artificial cuyas técnicas permiten a la máquina «aprender»). Estas técnicas aplicadas al trading permiten que los robots vayan mejorando la toma de decisiones, aunque la rentabilidad de dichas técnicas todavía está por probar en el mundo de las criptomonedas y están limitadas a gente con altos conocimientos estadísticos.

En los apartados anteriores hemos podido ver algunas de las estrategias más conocidas dentro del mundo del análisis técnico. Estas estrategias consisten siempre en dos pasos: reconocer una serie de condiciones y poner las órdenes adecuadas.

Como sabemos, aunque seamos capaces de reconocer las condiciones óptimas de compra, nadie nos asegura que podamos llevar a cabo las estrategias, ya que el tiempo cobra una vital importancia. Imaginemos exactamente el mismo caso que hemos visto en las medias móviles exponenciales. Esta estrategia consistía en poner una orden de compra cuando la media móvil de menor periodo cruzara de abajo a arriba a la media móvil de mayor periodo.

A simple vista parecía que si hubiéramos aplicado esta estrategia habríamos obtenido un beneficio de manera sencilla, pero volvamos a fijarnos en la imagen.



Si nos fijamos en el primer punto de cruce, aunque lo detectemos con tiempo, puede que realicemos una orden de compra por encima de la línea horizontal negra. A su vez cuando detectamos el segundo cruce puede que realicemos la venta por debajo de la línea horizontal. Esto significa que no solo no hemos aprovechado la estrategia, sino que hemos sufrido pérdidas al vender a un precio por debajo del valor de compra, y además hemos perdido las comisiones de compra y de venta.

Este ejemplo muestra la importancia de no solo tomar las decisiones

instantáneamente una vez hemos detectado ciertas condiciones, sino de analizar el mercado para poder establecer los precios óptimos de compra y de venta.

Además, debemos recordar que los exchanges permanecen abiertos 24 horas, por lo que puede que nuestras condiciones para vender se cumplan cuando estemos lejos del ordenador o incluso durmiendo. Por ello se hace imprescindible la necesidad de un robot que ejecute las órdenes de forma automática.

Algunos exchanges permiten establecer órdenes automáticas en base a unos parámetros preestablecidos. El problema suele ser que no se ofrece mucha flexibilidad en la variación de estos parámetros y, por lo tanto, seguimos en desventaja respecto a los robots particulares que son más personalizables y se pueden adelantar al hacer más lecturas del mercado.

Si, por ejemplo, un exchange me permite establecer una orden de compra cuando dos medias móviles se juntan, con un robot propio podría establecer una orden de compra cuando la distancia entre las mismas sea muy pequeña, de manera que me anticipo a todas las órdenes de compra que se ejecutarán una vez se toquen las medias móviles, de forma que aprovecho mucho más la subida de precios.

Otra de las ventajas de usar robots de trading es la posibilidad de realizar un backtesting de nuestra estrategia. En el capítulo siguiente veremos más en profundidad de qué se trata el backtesting y las ventajas que nos otorga.

### **5.2.5. *Backtesting***

Realizar un backtesting consiste en probar el modelo de trading con datos

históricos para calcular el beneficio que hubiéramos obtenido. Es de vital importancia realizarlo siempre antes de poner en funcionamiento un robot ya que, por un lado, comprobaremos si la estrategia es ganadora y, por otro, nos aseguraremos de que no haya fallos de programación que nos hagan pensar que la estrategia no sirve.

Para realizar este backtesting no es necesario que sepamos programar, ya que podemos usar herramientas como Excel para probar nuestra estrategia. Aunque también es cierto que si manejamos lenguajes de programación como R o Python el backtesting se realiza de forma mucho más rápida.

Además, también encontramos un pequeño problema en Excel y es que cuando intentamos hacer un backtesting con fórmulas pesadas en cientos de miles de líneas, puede que el ordenador necesite mucho tiempo para realizar los cálculos y existe la posibilidad de que el programa deje de funcionar. Por esta razón animamos a todo el mundo a aprender a programar en alguno de estos lenguajes o que consulte con algún especialista en la materia para realizar backtesting sólidos y confiables.

Queremos recordar, como mencionamos previamente, que el hecho de que, aunque nuestra estrategia sea ganadora en un backtesting, no podemos asegurar que vaya a ocurrir lo mismo en la realidad, ya que, en mercados de poca liquidez, puede que el precio de la criptomoneda sea distinto al que nosotros podemos comprar por una pequeña diferencia y esto haga que nuestra estrategia no sea tan buena como pensamos en un primer momento.

Recordemos que el precio de la criptomoneda se actualizará independientemente de la cantidad que se haya transaccionado, pudiendo encontrar que un precio ha

subido cuando en realidad a lo mejor se ha transaccionado un valor muy pequeño de dinero antes de volver al precio previo.

Estas últimas consideraciones cobran más importancia según reducimos el tiempo entre operaciones. Mientras que para estrategias a largo plazo no debemos preocuparnos por incluirlas en nuestro algoritmo, si estamos haciendo scalping, una diferencia de un 0,1% puede resultar crítica. En este último caso no debemos olvidar nunca incluir las comisiones en nuestros cálculos, ya que pueden hacer que una estrategia a priori rentable pierda dinero en la realidad.

#### **5.2.6. *Websockets y API REST***

Para poder entender en más profundidad el trading algorítmico, necesitamos conocer dos elementos importantes: los *websocket* y las API REST.

Un websocket es un protocolo de comunicación que permite establecer un canal de comunicación bidireccional sobre un socket TCP. Esta definición no es simple y requiere de conocimientos avanzados para entenderla, pero lo que nos interesa es para qué sirve dentro del mundo de las criptomonedas y el trading algoritmo.

Las casas de intercambio de criptomonedas más grandes suelen ofrecer el servicio de websocket, que no es nada más que una forma de comunicación de nuestro ordenador con la plataforma. Estos websockets nos enviarán toda la información del mercado en tiempo real.

Por ejemplo, cada vez que se produzca una transacción se nos enviará un mensaje con el precio de la misma, la cantidad y el tiempo en el que se ha

producido. Adicionalmente, se envía información relevante como es el par de monedas que estamos recibiendo, los decimales, etcétera.

A su vez, una REST API (Transferencia de Estado Representacional o *Representational State Transfer*) es una API (Interfaz de Programación de Aplicaciones o *Application Programming Interface*) que usa peticiones HTTP. Para explicarlo de forma sencilla, se trata de otra forma de comunicación con la plataforma de intercambio de criptomonedas. Gracias a esta comunicación podemos enviar peticiones de compra, venta, cancelaciones, etc., al exchange con el que estamos trabajando.

Gracias a los websockets tenemos toda la información del mercado en tiempo real y podemos construir todos los indicadores que creamos convenientes y programar las órdenes que queramos en base a nuestra estrategia de trading, para a continuación conectarnos mediante la API y hacer las peticiones de compra, venta, etcétera.

Una vez tengamos nuestra estrategia de trading creada ya podremos utilizar a nuestro robot de trading para comunicarse con la plataforma y operar de forma automática.

Es importante decir que, en la mayoría de los casos, si queremos usar un lenguaje de programación concreto, por ejemplo, Python o Java, necesitaremos usar algún *wrapper* externo. Gracias a estos wrappers nosotros podremos programar en el lenguaje que queramos y el wrapper se encargará de llamar a las subrutinas necesarias, es decir, transformará el lenguaje para nosotros.

Los wrappers son ajenos a las plataformas y debemos usarlos bajo nuestro propio riesgo. Gracias a la comunidad de criptomonedas, existen numerosos

proyectos en la plataforma GitHub de los que podemos ayudarnos.

Para poder conectarnos con la plataforma y poder utilizar nuestro robot en ella debemos disponer de una cuenta en la plataforma y generar lo que se conoce como una llave API o «API Key» y una contraseña o «API Secret» que usaremos dentro de nuestro código para permitir las compras, ventas o retirada de fondos.

Es importante señalar que cuando generamos una llave API en el exchange, se puede elegir los permisos que tendrá. Por ejemplo, podemos permitir que con las credenciales generadas solo se pueda operar, o podemos permitir que también se efectúen retiradas de fondos. Podemos generar diferentes llaves API con distintos permisos para aumentar la seguridad, o directamente no dejar permisos de retirada de fondos y hacerlos siempre a mano.

Cuando usemos plataformas que nos ofrezcan robots de trading, tendremos que introducir estas credenciales para poder utilizar su robot; en estos casos, solo aconsejamos permitir acceso a nuestra API a aquellas plataformas que sean respetadas por la comunidad y nunca otorgar acceso a una API con acceso a retirada de fondos a menos que contratemos un servicio que así lo requiera.

Otro aspecto importante a tener en cuenta si no queremos tener nuestro ordenador todo el día encendido operando con la plataforma es el alquiler de un servidor externo donde poder alojar nuestros robots y que esté conectado continuamente con la plataforma para poder operar día y noche.

Existen soluciones más profesionales como los servidores de Amazon o IBM que nos solucionan el problema de tener que tener nuestro ordenador siempre encendido y, además, agregan un valor añadido que es la seguridad que tendrán

nuestros robots de trading. Los servidores que nos ofrecen, a priori deberían tener más seguridad que nuestro ordenador personal y pueden ser una buena solución si también estamos preocupados porque nos puedan robar nuestros robots de trading.

A la hora de ver la rentabilidad de nuestro robot deberemos también tener en cuenta los gastos asociados a que esté conectado continuamente con la plataforma, tanto si lo hacemos con nuestro ordenador personal como si lo hacemos con un servidor externo. Deberemos hacer un balance para ver si sale rentable tener un servidor donde alojar nuestros robots o si, por el contrario, nos es más rentable tenerlos puestos en nuestro ordenador.

### **5.3. Gestión del riesgo**

En este capítulo vamos a ver diferentes apartados sobre la gestión del riesgo y cómo conseguir acotar en la medida de lo posible las pérdidas. Tan importante es tener una buena gestión del riesgo como una buena estrategia de trading.

Es muy importante la gestión del riesgo y pérdidas porque si no lo tenemos bien estructurado podemos perder todo el capital disponible para trading en poco tiempo. A continuación, os enseñaremos diferentes herramientas que nos ayudarán con esta tarea.

#### **5.3.1. Apalancamiento**

El apalancamiento financiero es una herramienta mediante la cual podemos tomar posiciones en el mercado con una cantidad de dinero mayor a la que disponemos; lo único que tenemos que tener es una fracción del total del dinero que estamos invirtiendo. Se puede definir como la relación que hay entre el dinero propio (capital propio) y el que nos prestan más el propio.

Es importante recalcar que el apalancamiento aumenta de forma significativa la exposición al riesgo. Podemos obtener rentabilidades enormes, pero también las pérdidas se multiplicarían, hasta llegar al punto de poder perder más dinero del depositado.

No recomendamos su uso hasta que no se hayan hecho muchas pruebas en simulación y se entienda bien cómo funciona este tipo de herramienta. Además, recomendamos que se utilice un capital que si lo perdemos no nos suponga un impacto significativo en nuestras finanzas. Y, obviamente, nunca pedir un crédito para hacer trading.

¿Cómo funciona el apalancamiento?

Supongamos que hemos estado siguiendo durante un tiempo a la empresa líder en tecnología en un determinado país y creemos que el precio de la acción se va a revalorizar para el próximo año. Así que nos decidimos a comprar acciones por valor de 100.000 €.

Nosotros solo disponemos de 10.000 € en el banco para comprar las acciones, así que tendremos que pedir un préstamo. Como ya teníamos 10.000 €, nos faltan 90.000 € que los saquemos de un préstamo con un tipo de interés del 10% anual. Como vamos a operar con 100.000 € y nuestro capital aportado solo han sido 10.000, el apalancamiento que estamos usando es 1:10 (por cada euro de

nuestro dinero estamos operando con 10).

Al cabo de un año, el valor de las acciones ha subido a 130.000 €, por lo tanto, devolvemos el préstamo de los 90.000 €, más los 9.000 € de interés y restamos los 10.000 € que pusimos de inversión propia, por lo que hemos conseguido 21.000 €. Es decir, que operamos con 10.000 € de dinero propio y hemos conseguido 21.000 € adicionales o, lo que es lo mismo, hemos obtenido un 210% de rentabilidad.

¿Qué hubiera pasado si no hubiéramos pedido el préstamo y hubiéramos operado solo con nuestros 10.000 €? Las acciones tendrían un valor de 13.000 € y solo hubiéramos ganado 3.000 €, es decir, hubiéramos conseguido una rentabilidad del 30%.

Como podemos observar, la rentabilidad al utilizar apalancamiento se ha multiplicado y es mucho mayor que si solo invirtiéramos con nuestro dinero, pero ¿qué pasaría si en vez de las acciones ir al alza hubieran ido a la baja?

Supongamos que las acciones después de un año valieran 80.000 €. Como pedimos prestados 90.000 € más los 9.000 € de intereses, debemos 99.000 €. Como el valor total de las acciones es 80.000 €, tenemos una pérdida total de 19.000 € de dinero prestado, más los 10.000 € iniciales que pusimos de nuestro dinero, es decir, unas pérdidas totales de 29.000 €.

Por eso mismo es muy importante saber utilizar esta herramienta, ya que podemos perder más de lo que hemos puesto como garantía, que en nuestro caso serían los 10.000 €. La práctica habitual de los brokers es liquidarte la posición si tus pérdidas van a superar la garantía depositada, para que no adquieras una deuda con ellos, pero en ocasiones, si no son capaces de cerrar tu posición lo

suficientemente rápido, te van a exigir más dinero del que tenías metido con ellos y de forma totalmente legal (por eso hay que leerse la letra pequeña siempre, os sonará eso de «las pérdidas ocasionadas pueden superar la garantía depositada»).

Pero, si tanto riesgo existe con el apalancamiento, ¿qué ventajas nos ofrece?:

- ▶ Multiplica la posible rentabilidad que tengamos en la operación.
- ▶ Ofrece la posibilidad de diversificar, ya que al solo necesitar una fracción del dinero total para invertir en una operación, podemos invertir en muchas más contando con el mismo capital.
- ▶ Tiene beneficios fiscales, ya que los intereses que se generen por la deuda que se adquiere se pueden deducir fiscalmente.

Resumiendo, el apalancamiento es una herramienta financiera complicada que puede ser de utilidad. Recomendamos que solo la uses si te dedicas profesionalmente a las inversiones y tienes muy claro los riesgos que conlleva, o si ya tienes mucha experiencia en el mundo de las inversiones y dominas esta herramienta, aunque sea en simulación.

### **5.3.2. Stop Loss**

Como ya te puedes imaginar después de todo lo que has leído en el apartado de trading, todos los traders pierden algunos de sus movimientos por muy buenos que sean. Es imposible tener un porcentaje de acierto del 100% y, por lo tanto,

como no se gana siempre es imprescindible acotar las pérdidas al máximo posible.

Lo que diferencia a los buenos traders de los malos es la gestión del riesgo y la gestión de las pérdidas. No es lo mismo tener una posible ganancia de un 5% y arriesgar un 1% de la cuenta que tener una posible ganancia del 1% y estar arriesgando el 5% de la cuenta.

Como se suele decir, corta muy rápido las pérdidas y deja correr las ganancias.

Pero ¿cómo hacemos esto? Para poder dejar correr las ganancias y cortar las pérdidas son interesantes estrategias como la de ir actualizando el Stop Loss (Stop Loss Dinámico). En el capítulo anterior estuvimos hablando de las ventajas que nos ofrecía tener unas pérdidas acotadas, pero, además, si lo vamos actualizando tenemos ventajas añadidas, por lo tanto, aconsejamos que se aprenda a usar el Stop Loss dinámico y que lo integremos en nuestra estrategia de trading para maximizar beneficios y minimizar pérdidas.

Aunque parece que tenemos programada la mente para hacer la técnica totalmente al revés y es que cuando vamos perdiendo dinero en una posición la solemos mantener pensando que en algún momento se revertirá el mercado y que podremos recuperar, y en cuanto ganamos algo queremos cerrar la posición y salirnos para obtener algo de beneficio no vaya a ser que el mercado cambie y perdamos lo poco que podíamos haber ganado. Inconscientemente queremos hacer justo lo contrario de lo que deberíamos hacer.

Muchas personas recomiendan el llamado Take Profit, que se trata de que en el momento que tengamos un beneficio fijado y lo conseguimos, cerramos la operación. Bajo nuestro punto de vista esto no es lo óptimo, y es mucho más

inteligente ir actualizando el Stop Loss, porque nos puede pasar muchas veces que nos perdamos una gran subida si, por ejemplo, tenemos puesto nuestro Take Profit a un 2% de beneficio. Como todos sabemos, hay operaciones (y más en criptomonedas) que pueden llegar a un 40% de beneficio en un día.

Saber cuándo retirar una posición y cuándo alargarla es importantísimo. No debemos aguantar una posición perdedora porque tengamos una corazonada de que en el futuro ese activo subirá. Es mejor tener unas pérdidas acotadas a tener pérdidas de un gran porcentaje del dinero total que disponemos.

Un consejo muy importante que damos cuando alguien se está iniciando en el trading (lleva pocos meses o algún año) es probar a hacer la operativa con poco dinero. En caso de que al perder varias veces y ver disminuir el capital le entren ganas de empezar a doblar las apuestas con la ilusión de empezar a ganar y recuperar el dinero perdido, entonces hay que parar en seco, dejar de hacer trading y replantearse todo desde el principio.

No puede guiar nuestra estrategia de trading el corazón, porque en ese caso perderemos todo nuestro dinero o gran parte de él de forma muy rápida. Así que, recuerda, es mejor ir actualizando el Stop Loss, cada vez que consigamos un 2% de beneficio lo aumentamos al precio actual menos un 1%, y de esta forma tenemos siempre acotadas las pérdidas y libres las ganancias.

Como ya os hemos hablado muchas veces a lo largo del libro, todas las estrategias de trading no son siempre las mejores para todos los traders. Utilizando esta en concreto sabiamente, podemos aumentar el retorno de nuestras inversiones, y aunque haya veces que en un posible trade no hayamos ganado todo lo que podíamos porque ha saltado el Stop Loss, tenemos que tener

en cuenta que, otras veces, gracias a que haya saltado esta herramienta hemos puesto a salvo nuestro capital y no hemos perdido una cantidad mayor.

Además, aconsejamos a la hora de hacer trading mirar las ganancias y las pérdidas en porcentaje. Ya que muchas veces nos juega una mala pasada para abrir o cerrar posición ver la ganancia o porcentaje de ganancia en dinero. Tenemos que tener en cuenta que si ganamos 200 € no lo tenemos que ver como el dinero que hemos ganado, si no lo que supone en porcentaje dentro de nuestra operación, ya que no es lo mismo si supone un 1% del total o si supone un 30%.

Por ejemplo, si hemos ganado 200 € pero eso supone un 0,1% del total, no habrá que cerrar la operación si pensamos que la subida es muy pequeña y que todavía puede subir más y, en cambio, si los 200 € que hemos ganado suponen un beneficio de un 40% lo más lógico es cerrar la operación o seguir con la estrategia de Stop Loss Dinámico para cuando cambie la tendencia del precio.

## **5.4. ¿Por qué es importante diversificar?**

Ahora vamos a tratar la importancia de tener diversificada nuestra cartera, para ello primero hablaremos de todas las ventajas que obtenemos al diversificar y, a continuación, pondremos un breve ejemplo con el que se entenderán todos los conceptos de forma fácil y sencilla.

Como ya habrás escuchado en otras ocasiones, es importante no tener todos los huevos metidos en la misma cesta, mejor tenerlos repartidos en varias, y esto se debe a que como dice el millonario inversor Warren Buffet «la diversificación es

protección contra la ignorancia». Esto quiere decir que es imposible que sepamos lo que va a ocurrir en los mercados y gracias a la diversificación podemos evitar o reducir las pérdidas en nuestra cartera en caso de que pase cualquier evento inesperado. Es fácil darse cuenta de que no hay ninguna inversión que sea completamente segura, y en caso de que existiera no sería rentable, por lo tanto, debemos proteger nuestro patrimonio diversificando.

Pero no solo es importante diversificar en los productos financieros, también es importante diversificar en los horizontes temporales, es decir, tener inversiones a corto, medio y largo plazo.

En cuanto a los productos financieros, podemos hablar de criptomonedas, acciones, ETF sobre índices bursátiles, fondos de inversión, etcétera.

Al hablar de horizontes temporales tenemos que tener claro cuánto tiempo queremos estar dentro de una inversión, por ejemplo, no es lo mismo invertir en una empresa incipiente que se dedica a la implantación de Blockchain (empresa en la que tendremos nuestro dinero inmovilizado durante posiblemente años esperando sacar unas ganancias muy elevadas), a invertir en una ICO, de la cual posiblemente nos salgamos en cuanto empiece a cotizar en algún exchange.

Además, dentro de la diversificación también encontramos diferentes niveles de riesgo que llevan asociados diferentes tipos de rentabilidad. Como es lógico, cuanto mayor riesgo estemos asumiendo mayor será la rentabilidad que podremos obtener en el futuro. No es lo mismo hacer una inversión en Bitcoin, que en un ETF sobre el SP500. Las rentabilidades que podemos esperar son totalmente distintas. Con el SP500 intentaremos proteger el capital y una pequeña revalorización anual, y con Bitcoin queremos conseguir una

rentabilidad de varios dígitos.

Por todo lo anterior es importante saber qué riesgo queremos asumir, los plazos a los que queremos realizar las inversiones y los productos con los que nos sentimos cómodos. Debemos saber que algunos productos son más difíciles de tener en cartera que otros y debemos conocer cuáles son los que nos interesan para saber cómo conseguirlos.

Muchas veces se piensa que la posibilidad de tener una cartera diversificada está condicionada a tener mucho capital para poder repartirlo en diferentes productos, y que no todas las personas se pueden permitir la diversificación, ya que no disponen de una cantidad elevada de dinero para la inversión y solo se podrían permitir uno, dos o tres productos financieros. Respecto a esto debemos decir que hay diferentes medios para poder diversificar adquiriendo un producto, y esto es, por ejemplo, un índice bursátil o un fondo de inversión. Por ejemplo, el exchange Huobi anunció la creación de su propio índice llamado Huobi 10, este índice consta de las 10 criptomonedas con mayor volumen de negociación enfrentadas al USDT de su plataforma. Por lo tanto, al adquirir una participación de este índice es como si estuviéramos comprando pequeñas participaciones de esas 10 criptomonedas.

Es interesante reseñar que los fondos de inversión surgieron por la necesidad de diversificar las inversiones, y por la comodidad que representan para el pequeño inversor, ya que al invertir en uno de ellos está diversificando directamente entre todos los productos que componen a ese fondo de inversión.

Además, una ventaja de la inversión en un índice es que no hay que hacer un seguimiento activo de la cartera, ya que se encargan los que lo han creado de

hacer la ponderación de pesos de cada uno de los productos que lo componen, así como del rebalanceo de los activos. De esta forma se consigue que el pequeño inversor se despreocupe de esa inversión y tenga a su vez su dinero diversificado, protegiéndose de los diferentes riesgos intrínsecos de los activos.

Beneficios de tener una cartera diversificada:

- ▶ Proteger el patrimonio de cualquier evento inesperado.
- ▶ Tener cubiertos diferentes horizontes temporales de inversión.
- ▶ La posibilidad de vender los productos que más rentabilidad nos hayan otorgado para conseguir liquidez, y minimizar la posibilidad de que tengamos que vender algún producto financiero en pérdidas porque necesitemos liquidez.

Recordemos que la diversificación, en caso de que solo se vaya a realizar comprando criptomonedas, es importante porque:

- ▶ Disminuimos el riesgo de tener una sola criptomoneda. En caso de que hiciéramos una apuesta fuerte por una criptomoneda y luego tuvieran fallos con el proyecto, fallos en la seguridad, prohibiciones de algún gobierno, etc., se podría dar el caso de que perdiéramos todo nuestro dinero o, en el mejor de los casos, un alto porcentaje de este. Por eso mismo es importantísimo diversificar entre diferentes criptomonedas, aunque la rentabilidad pueda bajar en caso de que hubiéramos apostado desde el principio por la criptomoneda ganadora.
- ▶ Promediamos la rentabilidad que nos otorgan las criptomonedas. Es posible que alguna criptomoneda de las que tengamos en cartera pierda un pequeño

porcentaje de su valor y otra de las que tenemos lo compense.

- Podemos definir el nivel de riesgo que queremos asumir, por ejemplo, podemos tener en cartera criptomonedas asentadas y con larga trayectoria como Bitcoin y Ethereum y además varias criptomonedas incipientes con un peso menor en la cartera para minimizar el riesgo.

Debemos tener en cuenta que si lo que queremos es maximizar el beneficio (maximizando a su vez el riesgo) lo que podemos hacer es invertir en ICO o invertir en las monedas nuevas que aparezcan en CoinMarketCap, siempre y cuando tengamos en cuenta el proyecto que tienen detrás, si es realizable o no, si el equipo es competente, etc. Si pensamos que todo lo anterior ocurrirá, quizás podamos esperar que tenga un aumento de precio muy significativo y que podamos multiplicar la inversión inicial que hicimos.

Es importante recordar que no siempre las inversiones que se realizan salen como nosotros esperábamos, por tanto, debemos hacer una gestión inteligente de nuestro patrimonio por si ocurriera un escenario desfavorable. Recomendamos que solo se utilice el dinero que se tenga disponible y que no se necesite, es decir, que «no nos importe perder». Ya sabemos que a todo el mundo le importa perder su dinero, pero con esto nos referimos al dinero que no le suponga un problema perder, es decir, nunca el dinero de hipoteca, alimentación, etcétera.

También recomendamos no endeudarse ni pedir dinero prestado para hacer inversiones, ya que, como hemos dicho muchas veces, no sabemos a ciencia cierta cómo va a salir nuestra inversión y podría darse el caso de perder el capital que nos han prestado y seguir teniendo la deuda. También es importante recalcar que, en caso de que hayamos perdido dinero con las inversiones, la fórmula de

doblar lo invertido a ver si nos recuperamos no suele funcionar y suele traer una desgracia mayor. Por lo tanto, te volvemos a recordar que solo inviertas el dinero que no te importe perder y que hagas una gestión inteligente del patrimonio.

Para entender mejor todo esto vamos a poner un ejemplo:

Supongamos que tenemos tres escenarios diferentes y en cada uno de ellos invertimos 20.000 €. En el primer escenario solo hemos comprado una criptomoneda y, por lo tanto, no hemos diversificado nada la inversión. En el escenario B hemos comprado 5 criptomonedas; y para el escenario C hemos comprado 10 criptomonedas, por lo tanto, los escenarios B y C están diversificados, estando más diversificado el C. Tanto para el escenario B como para el escenario C hemos repartido el dinero dando el mismo peso e importancia a cada una de las criptomonedas, por lo tanto, en el escenario B compramos 4.000 € de cada una de las criptomonedas y en el escenario C compramos 2.000 € de cada criptomoneda:

- ▶ Escenario A: Nuestra cartera está compuesta por IOTA.
- ▶ Escenario B: Nuestra cartera está compuesta por IOTA, Litecoin, Ethereum, Neo y Stellar (4.000 € en cada criptomoneda).
- ▶ Escenario C: Nuestra cartera está compuesta por IOTA, Litecoin, Ethereum, Neo, Stellar, Monero, Storj, Poet, ICON y Nano (2.000 € en cada criptomoneda).

Imaginemos para los tres escenarios que, al minuto siguiente de haber comprado las criptomonedas, aparece una noticia en la comunidad de que el equipo de IOTA ha tenido un problema interno de seguridad. Debido a esta noticia la

comunidad se pone nerviosa y empieza a vender los IOTAS que tiene porque no sabe la gravedad del problema y hay miedo de perder el dinero de la inversión. Al haber pánico por la noticia y la gente empezar a vender sus IOTA, baja el precio de la criptomoneda un 40%.

- Escenario A. Como toda nuestra cartera se compone de IOTA, acabamos de perder el 40% del valor total de la cartera, por lo tanto, hemos perdido en muy poco tiempo 8.000 €.

Valor total de nuestra cartera = 12.000 €

- Escenario B. Todas las criptomonedas que tenemos en cartera tienen el mismo valor a excepción de IOTA. En este caso, IOTA representa una quinta parte de nuestra cartera (20%) por lo tanto solo hemos perdido el 40% de esa quinta parte de los 20.000 € iniciales.

$$\text{valor perdido por IOTA} = 20.000\text{€} \times \frac{40}{100} \times \frac{20}{100} = 1.600\text{€}$$

Valor total de nuestra cartera = 18.400 €

- Escenario C. Todas las criptomonedas que tenemos en cartera tienen el mismo valor a excepción de IOTA. En este último caso, IOTA solo representa una décima parte de nuestra cartera (10%). Hemos perdido el 40% de esa décima parte de los 20.000 € iniciales.

$$\text{valor perdido por IOTA} = 20.000\text{€} \times \frac{40}{100} \times \frac{10}{100} = 800\text{€}$$

Valor total de nuestra cartera = 19.200 €

En estos tres escenarios tenemos pérdidas de 8.000, de 1.600 € y de 800 €. La diferencia es considerable.

Es importante recalcar que diversificar la cartera no es tener en nuestra cartera 100 criptomonedas diferentes, sino un número óptimo con el que veamos que sufrimos menos riesgos y que pueda potenciar la rentabilidad que obtengamos en el futuro

## **5.5. Rebalancear la cartera**

En este capítulo vamos a hablaros de la importancia de rebalancear nuestra cartera.

Rebalancear la cartera simplemente es volver al porcentaje inicial de inversión que otorgamos a cada uno de nuestros activos.

Vamos a verlo con un ejemplo con números para que quede más claro.

Supongamos que tenemos 10.000 € para invertir en criptomonedas y decidimos que nuestra cartera la queremos diversificar en cinco criptomonedas. Estas criptomonedas serán Ethereum, Litecoin, Bitcoin, IOTA y Stellar. Así que asignaremos a cada una de ellas el 20% del dinero total que disponemos, es decir, 2.000 €.

Al día siguiente, consultamos nuestra cartera y comprobamos que los porcentajes que tienen cada una de nuestras criptomonedas han variado y ya no tienen el 20% inicial que tenían cada una de ellas.

A día de hoy nuestra cartera ha variado en precio total (ha subido el valor total

de la cartera) y además tenemos que el precio del Bitcoin y de Stellar ha bajado, y ahora representan en nuestra cartera un 17% y un 15% respectivamente (el precio de Stellar ha bajado más que el del Bitcoin), la criptomoneda Litecoin sigue con un precio similar al día anterior, pero hoy solo representa un 19% en vez de un 20% (esto se debe a que se ve influenciada por el valor total de nuestra cartera, que como ayer teníamos 2.000 € de 10.000 € representaba el 20%, pero hoy como nuestra cartera ha aumentado de valor, esos 2.000 € que tenemos en Litecoin solo representan un 19% de la cartera), y, por último, tenemos Ethereum y IOTA con un 25% y un 24 % respectivamente (Ethereum ha subido más que IOTA).

Como hemos podido comprobar en el ejemplo, simplemente en un día nuestra cartera ya no está con la ponderación de criptomonedas que queríamos, y, por tanto, ya no tenemos el riesgo diversificado según la estrategia que queríamos seguir en un principio.

Por todo esto es muy importante rebalancear nuestra cartera y tener siempre (en la medida de lo posible) el porcentaje de criptomonedas que hemos decidido en un primer momento. Para esto, tendremos que vender las criptomonedas que más hayan subido y compraremos las que más hayan bajado.

Así que rebalancear simplemente es devolver la cartera con la que estamos invirtiendo a su distribución inicial.

Gracias al reequilibrio de cartera conseguimos que la alta volatilidad de los mercados nos afecte lo menos posible y seguir con la estrategia de inversión que decidimos en un primer momento.

Otra de las grandes ventajas del rebalanceo es que, en muchas ocasiones, se

consiguen rentabilidades más elevadas que si solo hubiéramos comprado nuestros activos al principio y nunca los hubiéramos rebalanceado. Esto se debe a que cuando rebalanceamos nuestra cartera lo que estamos haciendo es vender los activos que tenemos en cartera que han aumentado su precio y comprar los activos que han bajado de precio. En otras palabras, nos beneficiamos de la volatilidad del mercado, que tiende a sobre reaccionar tanto en las subidas como en las bajadas. Aprovechando esta situación, vendemos cuando hay un optimismo irracional, y compramos cuando hay un pesimismo injustificado. Por supuesto que tenemos que tener en cuenta que algún activo puede haber sufrido un deterioro permanente y nos tendríamos que deshacer de él, o compraríamos más y más de un activo que tiende a cero.

Para rebalancear la cartera, aparte de la posibilidad de vender y comprar los activos que necesitemos hasta llegar a nuestra distribución ideal, también podemos invertir más dinero y comprar los activos que hayan bajado de nuestra cartera. Esta opción es igual de válida que la anterior, pero tenemos que ser conscientes de que estamos aumentando la inversión que hacemos y tendremos que rehacer el cálculo de nuestra cartera en base al precio que tiene y al que estamos sumando con la última aportación.

Es importante que, también, para la forma de rebalancear la cartera sin invertir dinero y solo teniendo en cuenta los activos que han subido y han bajado, y el porcentaje que representan en nuestra cartera, tenemos que mirar el precio total actual de la cartera. Es decir, en nuestra cartera el valor inicial que teníamos era de 10.000 €, pero puede que ahora el valor total sea de 9.500 € o de 10.500 €, por eso mismo tenemos que saber el valor total y con ese valor calcular el dinero que representa el porcentaje que queremos de los activos. Por ejemplo, en el

caso de 9.500 €, un 20% serán 1.900 €, y en el caso de 10.500 € serán 2.100 €.

## **Conclusión**

Con esto acaba el capítulo de trading. Esperamos que os haya ayudado a entender de forma sencilla en qué consiste esta actividad. Siempre que se ve algo nuevo desde fuera parece extremadamente complejo. Pero, como pasa con todas las disciplinas, si empezamos paso a paso, todo tiene mucho más sentido. Solo hay que saber cómo unir las piezas del puzzle.

Gracias al trading, miles de aficionados han conocido el mundo de las criptomonedas y posiblemente eso provocara la explosión de precios que vimos a finales de 2017. Lo importante de todo esto no es el precio que tengamos ahora en los mercados, sino que, gracias a esa entrada masiva de usuarios, a día de hoy prácticamente todo el mundo ha escuchado la palabra bitcoin.

Y esto es todo. Escribir este libro ha sido toda una aventura. Los días pasan volando mientras investigas contenido, redactas una y otra vez párrafos que no terminan de convencerte, y cambias el orden de los capítulos hasta que todo parece tener un orden lógico. Es un proceso iterativo que parece no terminar nunca.

Durante este periodo de tiempo hemos visto cómo se ha desinflado ligeramente el interés en esta tecnología, a la vez que soluciones reales basadas en ella tocan los mercados. Se puede comprar un bitcoin por poco más de 3.000 dólares, y un ether cotiza por debajo de los 90 \$. Todos sabemos que los mercados tienden a sobrerreaccionar, lo vimos en diciembre de 2017, y puede que estemos viviéndolo ahora en diciembre de 2018. Solo con el tiempo sabremos si esto quedará en una mera anécdota, o si seguirán cayendo sus cotizaciones mucho más.

De lo que si estamos convencidos es que la tecnología ha llegado para quedarse.

Pero todo llega a su fin. Nuestro objetivo al escribir este libro era lograr que cualquier persona que no conozca la tecnología blockchain pueda terminarlo y sentir cierta satisfacción por haber sido capaz de comprender el contenido.

De ser así, habremos cumplido con la meta que nos marcamos cuando comenzamos su redacción.

Esperamos que hayáis disfrutado de la lectura.

# GLOSARIO

**Altcoin:** Alternative to Bitcoin, son otras criptomonedas cuyo fin es intercambiar valor.

**Bitcoin:** Primer caso de dinero digital entre pares sin necesidad de una autoridad central que controle que se produce el intercambio.

**Blockchain:** Tecnología subyacente de las criptomonedas. Es una forma de almacenar información distribuida, descentralizada y segura.

**Bloque:** Un conjunto de transacciones que se agrupan y se validan criptográficamente para que pasen a formar parte de la cadena.

**Clave privada:** La clave que se utiliza para desbloquear los fondos de una cartera y enviarlos a otra dirección. Nunca se debe de compartir.

**Clave pública:** Es la dirección que podemos compartir para que nos envíen criptoactivos. Sería como compartir nuestra dirección de correo electrónico.

**Criptografía:** Técnicas de cifrado que tratan de impedir que nadie pueda entender una información excepto el destinatario.

**Criptomoneda:** Moneda digital de uso entre pares.

**Cypherpunk:** Movimiento que defiende el uso de la encriptación para preservar la privacidad del individuo frente a gobiernos y corporaciones.

**Doble gasto:** Equivalente a la falsificación del dinero tradicional. Consiste en el

intento de gastar más de una vez una moneda digital.

Ethereum: Plataforma que permite el despliegue de Smart contracts.

Exchange: Plataforma donde compramos y vendemos criptoactivos.

Fiat: Es el dinero tradicional, y su valor está respaldado legalmente por un gobierno.

Fomo: Fear Of Missing Out, o temor a quedarse fuera. Es una táctica de marketing que intenta producirte una sensación de urgencia para que compres impulsivamente.

Fud: Fear, Uncertainty, Doubt. Miedo, incertidumbre, duda. Consiste en extender rumores (con fundamento, o no) para dañar la imagen de un proyecto o persona.

Hard fork: Bifurcación contenciosa de una blockchain. Cuando los participantes no se ponen de acuerdo en cómo debe evolucionar la tecnología, pueden producirse dos versiones distintas de un protocolo.

Hash rate: Medida de la potencia informática destinada al minado de una criptomoneda basada en Proof of Work.

Hold (o Hodl): Mantener en cartera una criptomoneda y no venderla, aunque haya malas noticias.

Hype: Sobreexcitación o nerviosismo ante un evento.

ICO: Initial Coin Offering. Consiste en la venta de un token para interactuar con una plataforma basada en blockchain y que los promotores del proyecto se puedan financiar.

KYC: Know Your Customer. Es una directiva para evitar el blanqueo de

capitales que requiere que se identifique al comprador.

Minar: Validar criptográficamente un bloque de una blockchain para anexarlo a la cadena.

Nodo: Participante en una red p2p que está ejecutando el software del protocolo.

PoS: Proof of stake o prueba de participación. Es una forma de validar bloques poco intensiva en recursos informáticos, que requiere que se bloqueen criptomonedas.

PoW: Proof of work o prueba de trabajo. Es una forma de validar bloques intensiva en recursos informáticos.

Pump & dump: Esquema en el que unos pocos participantes animan a comprar a mucha gente una criptomoneda en un espacio corto de tiempo, para que suba su cotización. Mientras sube, los promotores estarán colocando la criptomoneda comprada por ellos anteriormente a los participantes.

Satoshi: Unidad mínima divisible de un bitcoin.

Satoshi Nakamoto: Pseudónimo del creador de Bitcoin.

Scam: Timo.

Shitcoin: Criptomoneda sin valor ninguno, que no aporta ventajas frente a otros protocolos más utilizados.

Timestamp: Sello de tiempo, marca el momento en el que un evento ha tenido lugar para garantizar el orden en el que los sucesos han tenido lugar e impedir su alteración.

Token: Criptoactivo que representa un derecho de acceso, de votación, sobre beneficios...

TPS: Transacciones por Segundo.

Trading: Actividad de compra y venta de un activo.

Wallet: Cartera, es donde se alojan los criptoactivos.

Wei: Unidad mínima divisible de un ether.

Whitepaper: Documento técnico que aborda qué problema se busca resolver y cómo se va a hacer tecnológicamente.

- [1] <https://coinmarketcap.com/>
- [2] <https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html>
- [3] <https://www.activism.net/cypherpunk/manifesto.html>
- [4] <https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html>
- [5] <https://www.blockchain.com/es/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b>
- [6] <https://www.blockchain.com/es/btc/block/00000000839a8e6886ab5951d76f411475428afc90947ee320161bl>
- [7] <http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate>
- [8] <https://bitcointalk.org/index.php?topic=20.0>
- [9] <https://bitcointalk.org/index.php?topic=137.0>
- [10] <https://news.slashdot.org/story/10/07/11/1747245/bitcoin-releases-version-03>
- [11] <https://bitcointalk.org/index.php?topic=823.0>
- [12] <https://bitcointalk.org/index.php?topic=823.0>
- [13] <https://bitcointalk.org/index.php?topic=1306.0>
- [14] <https://bitcointalk.org/index.php?topic=1672>
- [15] <https://www.linkedin.com/in/rossulbricht/>
- [16] <https://freeross.org/making-a-murderer/>
- [17] [https://freeross.org/wp-content/uploads/2018/07/Doc\\_14\\_Dismissal\\_Indictment\\_7-26-2018.pdf](https://freeross.org/wp-content/uploads/2018/07/Doc_14_Dismissal_Indictment_7-26-2018.pdf)
- [18] Los pools tienen la función de agregar la capacidad de cálculo de varios mineros para tener más posibilidades de resolver un bloque, a costa de compartir la recompensa entre todos los participantes.
- [19] [https://en.bitcoin.it/wiki/Mt.\\_Gox](https://en.bitcoin.it/wiki/Mt._Gox)
- [20] <https://www.recode.net/2018/1/22/16911692/cryptocurrency-bitcoin-trading-coinbase-revenue-secondary>
- [21] <https://www.cbinsights.com/research/report/coinbase-strategy-teardown/>
- [22] [https://en.wikipedia.org/wiki/Mt.\\_Gox](https://en.wikipedia.org/wiki/Mt._Gox)
- [23] <https://es.scribd.com/doc/209050732/MtGox-Situation-Crisis-Strategy-Draft>
- [24] <https://www.bloomberg.com/news/articles/2018-01-11/world-s-top-ranked-crypto-venue-added-240-000-users-in-one-hour>
- [25] <https://bitcoin.org/bitcoin.pdf>
- [26] <https://twitter.com/cburniske/status/896375943736020993>
- [27] <https://www.bloomberg.com/news/articles/2018-07-16/happy-prime-day-jeff-amazon-ceo-s-net-worth-tops-150-billion>
- [28] Capitalizaciones a 13 de septiembre del 2018.

- [29] <https://www.visa.com/blogarchives/us/2013/10/10/stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/index.html>
- [30] <https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#1y>
- [31] <https://lightning.network/lightning-network-paper.pdf>
- [32] [https://en.bitcoin.it/wiki/Hashed\\_Timelock\\_Contracts](https://en.bitcoin.it/wiki/Hashed_Timelock_Contracts)
- [33] <https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf>
- [34] <https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html>
- [35] [https://es.wikipedia.org/wiki/Turing\\_completo](https://es.wikipedia.org/wiki/Turing_completo)
- [36] <http://paper.gavwood.com/>
- [37] <https://www.usv.com/blog/fat-protocols>
- [38] <https://www.ecb.europa.eu/ecb/tasks/monpol/html/index.es.html>
- [39] <https://www.forbes.com/sites/laurashin/2018/01/02/meet-the-crypto-billionaires-getting-rich-from-ripples-xrp/#2e594e1c3289>
- [40] <https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md>
- [41] <https://tether.to/>
- [42] <https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/>
- [43] <https://cointelegraph.com/news/canceled-audit-and-issuance-of-300-mln-new-tokens-whats-going-on-with-tether>
- [44] [https://www.binance.com/resources/ico/Binance\\_WhitePaper\\_en.pdf](https://www.binance.com/resources/ico/Binance_WhitePaper_en.pdf)
- [45] <https://www.cnbc.com/2018/04/03/floyd-mayweather-backed-cryptocurrency-ico-fraud-sec-says.html>
- [46] Tipo de ataque en el que se suplanta la identidad de un agente como podría ser nuestro banco, para engañarnos y que le demos al atacante nuestras claves y nos pueda robar los fondos.
- [47] Programa malicioso que graba todo lo que tecleamos y lo envía al atacante, de esta forma puede robar nuestras contraseñas.
- [48] <https://www.cnbc.com/2017/12/20/man-lost-127-million-worth-of-bitcoins-and-city-wont-let-him-look.html>
- [49] <https://blog.chainalysis.com/reports/money-supply>