Introducción

Desde la llegada del Bitcoin en 2008, la tecnología ha evolucionado mucho. Primero se escindió en lógica permisionada y no permisionada, luego más recientemente, los componentes técnicos han evolucionado tanto que el paradigma de cadena de bloques tiende a perder su sentido.

La hipotética llegada de las aplicaciones descentralizadas que dan lugar a empresas autónomas no ha visto la luz. La ambición de los usos y de la técnica también parece alejarse de estos ideales.

Sin embargo, los especialistas tecnológicos y los usuarios de las nuevas variantes de blockchain siguen teniendo que enfrentarse a los mismos desafíos. Estos últimos se dividen en desafíos técnicos y experiencias primerizas. El aspecto legal es especialmente delicado, sobre todo porque algunas blockchains son internacionales por naturaleza. Por último, analizaremos los desafíos específicos o híbridos del código abierto, de las bifurcaciones, de la volatilidad de las criptomonedas y del mal uso de la tecnología.

# Desafíos técnicos

De todos los desafíos, los desafíos técnicos son seguramente los más apasionantes para los especialistas. Por ejemplo, de todas las arquitecturas imaginables, la de par a par es preferible con diferencia por sus cualidades de resiliencia. Sin embargo, solo se aplica en raras ocasiones porque es muy difícil garantizar la confianza. Gracias a la tecnología de registro descentralizado, la confianza está intrínsecamente vinculada con el sistema encriptado. No obstante, esta confianza tiene un coste y presenta dificultades técnicas nada despreciables.

## **1. Unificación de blockchains y ejecución de contratos**

La primera dificultad consiste en la estructura misma de una cadena de bloques. Por ejemplo, tomemos la cadena propuesta por la fundación Ethereum y la cadena ya larga del protocolo Bitcoin. En el estado actual de la tecnología, no hay solución para hacer converger dos cadenas. En términos biológicos, sería como pedirles a dos felinos procedentes de un árbol genético que se separó hace millones de años, que se reproduzcan entre ellos. En el caso de la biología, parecería que todos los seres vivos comparten los mismos componentes fundamentales. En cuestión de blockchain, incluso esta idea es infundada.

A corto plazo se derivan dificultades evidentes de validación. Una aplicación descentralizada puede evolucionar en una blockchain donde se han hecho modificaciones menores, pero no en otra blockchain. Así, podemos citar la ligera divergencia entre las soluciones Ethereum y Quorum. Por el contrario, la información contenida en un bloque de la tecnología IOTA no se corresponde en casi ningún aspecto con la contenida en un bloque Ethereum. En teoría, necesitaríamos una tabla de correspondencia, o diccionario, para transponer una aplicación de una cadena a otra. En último término, esto daría como resultado tener un equivalente de cadena única. Se han puesto en marcha algunos proyectos para resolver este problema. Por ejemplo, podemos hablar de *Bancor* en las blockchains públicas o incluso *Hyperledger Burrow* en las blockchains permisionadas. Estos proyectos están básicamente en la fase de prototipos. El uso de API con un almacenamiento en espejo de los tokens es la única solución propuesta.

Más allá de los tokens, la gestión de los activos digitales todavía está en una fase embrionaria.

Por lo tanto, actualmente no existe una tabla de correspondencia entre blockchains de estas características, y es muy poco probable que exista en pocos años porque se enfrenta a grandes dificultades. En un mundo perfecto, una sola cadena sería suficiente para capturar toda la información que deseamos conservar. Solamente, en el caso de una cadena Bitcoin, por ejemplo, el aspecto no Turing completo impide la captación de cierta información, aunque las cadenas Ethereum o Hyperledger se hacen cargo de ella con facilidad. Por otro lado, la reciente divergencia del concepto de blockchain hace que el futuro sea aún más incierto.

## **2. Pérdida o corrupción de claves de acceso**

La estructura del registro descentralizado y del proceso de almacenamiento permite que un objeto dado sea compartido entre dos partes. El problema recurrente afecta a las personas que han perdido su clave de cifrado privada.

Algunas empresas se han organizado para conservar estas claves en cajas fuertes digitales. Por ejemplo, podemos recordar la solución *Ledger*, que permite almacenar las claves en un soporte físico.

También existe la posibilidad de recuperar la clave mediante una cadena de palabras generadas aleatoriamente, sin embargo, no siempre es posible retirar los derechos sobre una carpeta (wallet) cuando la clave se ha corrompido. Tampoco hay último recurso, como suele haber cuando se trabaja con un administrador del sistema informático.

## **3. Acceso a los datos y purga**

En el marco de una transferencia de objetos (imágenes, archivos, aplicaciones, etc.), el objeto raramente se integra en una blockchain. Por el contrario, su hash se envía a la blockchain, y el documento se almacena en una solución off-chain. Es posible encriptar el archivo, pero la lógica de acceso puede ser suficiente para proteger el acceso.

Si se pierde la clave de acceso, el archivo es inaccesible, virtualmente para siempre. La única manera de recuperar esta clave en una blockchain pública son las soluciones que ya hemos mencionado antes.

En el contexto de una blockchain de consorcio, la solución también estar bien diseñada para protegerse de este caso extremo.

Así, los archivos y los fondos acumulados en una red pueden convertirse en inaccesibles o inutilizables para siempre. En 2019, se almacenaron muchos millones en una blockchain como consecuencia del éxito de una ICO. El problema fue que el fundador de la blockchain y único poseedor de las claves de encriptado murió prematuramente, sin facilitar ningún mecanismo de reversibilidad.

Esta dificultad suscita otra. ¿Cómo purgar la información obsoleta u olvidada en una red? Como la tecnología se basa en un almacenamiento descentralizado virtualmente infinito, es imposible hacer limpieza, aunque sea necesario a más largo plazo.

Hay soluciones a nivel de una blockchain permisionada. Para Hyperledger, por ejemplo, se crea una cadena nueva por intervalo de tiempo y se destruyen las antiguas de manera progresiva.

## **4. Consumo energético y cálculos inútiles**

El consumo energético es un gran problema de la tecnología. El sistema blockchain se base en un proceso de verificación de una cadena binaria específica y única para cada bloque. Sin embargo, a una unidad de cálculo sola, como un servidor multinúcleo, le costaría décadas, como mínimo, validar un bloque en la cadena. Añadir miles de millones de unidades de cálculo en paralelo permite reducir significativamente el tiempo de cálculo, hasta tal punto que la resolución tarda una media de 10 minutos en la cadena Bitcoin.

Las últimas versiones de blockchain (p. ej.: EOS) no consumen casi nada en cuanto a energía. Las blockchains permisionadas parecen responder igualmente y de manera progresiva a esta limitación. Así, a excepción del bitcoin, la tecnología consume cada vez menos energía. Incluso Ethereum tiene previsto cambiar su algoritmo de consenso para responder a la urgencia del consumo energético asociado a la tecnología.

## **5. Calidad de los desarrollos**

Los protocolos más conocidos actualmente todavía no parecen haber sido pirateados. En cambio, la lógica de los smart contract que funcionan en estas plataformas han sido presa de numerosos ataques que han tenido éxito.

La naturaleza código abierto de algunos códigos hace que, por naturaleza, sean más fáciles de piratear, porque es visible el funcionamiento del código en sí mismo. En el contexto de las blockchains públicas, un smart contract que tiene un fallo es especialmente problemático, sobre todo si otra sección de código lo reutiliza. En efecto, pone en peligro toda la cadena que utiliza este programa.

En el caso de las blockchains permisionadas, los smart contracts (o chaincodes) han visto una fuerte disminución de su impacto para reducir el riesgo de un efecto bola de nieve.

En conjunto, el sector ha evolucionado mucho y hay herramientas a disposición de los desarrolladores y de los especialistas técnicos. Podemos citar, por ejemplo, las cajas de Petri, la prueba formal o incluso la PCP (*probabilistic checkable proof*, Prueba probabilísticamente verificable) para reducir el riesgo técnico que acompaña a un smart contract. Muchas blockchains implementan la prueba formal de manera predeterminada, para proteger a los usuarios del código. Por último, hay analizadores de bytecode a disposición de los desarrolladores con la finalidad concreta de verificar cuatro fuentes habituales de errores, vamos a verlas:

* las dependencias de orden de transacciones;
* las dependencias de la marca de fecha y hora;
* las excepciones mal gestionadas;
* las vulnerabilidades de reintroducción.

Por ejemplo, el error de reintroducción constatado en el programa TheDAO, ha permitido que en un solo día un individuo desvíe muchas decenas de millones de euros en su equivalente en criptomoneda.

## **6. Distribución de la potencia de cálculo**

La distribución de la potencia de cálculo y su uso son problemas reales para muchas blockchains. Técnicamente, se deben validar todas las transacciones para integrarlas en la cadena.

Cuando un dato que se desea insertar entra en conflicto con otro (p. ej.: varias ramas de una misma cadena), se establecen mecanismos de filtrado y de tratamiento preferencial. Por ejemplo, en el protocolo Bitcoin tiene prioridad el dato sobre la cadena más larga. De lo que resulta que el grupo de interés que dispone de más del 51 % de la potencia de cálculo tiene superpoderes y es capaz de escribir en la cadena más o menos todo lo que quiere. Esta cuota se reduce significativamente con el planteamiento de la prueba de participación.

Aunque esta vulnerabilidad es conocida, desde la llegada de la primera blockchain Bitcoin en 2008, parece que por el momento no se ha observado su uso, solo durante algunos minutos. En cambio, hay que observar muy de cerca la potencia de cálculo en China específicamente desplegada para validar transacciones. En unos años, el peso de China en la validación de transacciones en la red Bitcoin ha aumentado hasta alcanzar aproximadamente el 50 %. Para corromper el sistema de validación, habría que obligar a las empresas especializadas en la validación de transacciones de la blockchain deseada, a validar una transacción falsa. Eso corrompería su fuente de ingresos y cortaría la rama en la que están asentadas.

Esta debilidad es permanente y cada vez más molesta para los protocolos nuevos.

## **7. Velocidad de transacción y evolución**

En teoría, una transacción se ejecuta y valida en 10 minutos, que transcurren desde el momento de su publicación hasta el momento de su inclusión en la cadena Bitcoin. En la práctica no se ha visto algo así. El protocolo Bitcoin, uno de los más utilizados, sufre graves problemas de congestión del sistema. Para validar una transacción pueden pasar desde varias horas hasta varios días. El problema no está tan relacionado con la potencia de cálculo como con la cantidad de transacciones que se pueden gestionar de manera simultánea.

Las redes Visa y MasterCard pueden hacerse cargo de muchos miles de millones de transacciones por segundo. Lo que puede gestionar la red Bitcoin se cuenta por unidades. La red Bitcoin ha propuesto métodos de mejora como Lightning, o incluso aumentar el tamaño de un bloque. Estas mejoras no resuelven el problema de fondo. En la práctica, la red está por naturaleza al límite de su capacidad de creación de bloques. Añadir potencia de cálculo no acelera el proceso de minado.

La red Ethereum parece experimentar las mismas dificultades. Por ejemplo, a finales de 2017, hizo furor una aplicación llamada Cryptokitties, hasta el punto de representar casi el 25 % del tráfico en la plataforma. El atasco era lo suficientemente importante para que costara semanas validar una transacción.

Bitcoin y Ethereum se han enfrentado a un pico de actividad mientras uno de los vectores clave de la explosión de las ICO y de las nuevas tecnología se limitaba a comparar la cantidad de transacciones por segundo. Siempre tomando como referencia la red de pago mediante tarjeta bancaria, se habían hecho promesas muy ambiciosas. Para alcanzar este objetivo empezó una carrera frenética, e incluso se rebajó la definición de una transacción y de su contenido. Los nuevos planteamientos se decantaron por cambiar radicalmente de enfoque y eligieron consensos más laxos en materia de seguridad, pero mucho más eficientes en velocidad de tratamiento.

A mediados de 2019, una cierta cantidad de tecnologías permiten alcanzar récords de eficiencia, con más de 10 000 transacciones por segundo. Sin embargo, la complejidad de los elementos intercambiados (activos digitales) todavía es muy limitada. La tecnología progresa a un ritmo inesperado y todavía quedan muchas líneas de mejora posibles para crear un sistema realmente descentralizado. Las blockchains permisionadas progresan con rapidez y algunas de ellas ya están preparando la integración de manera nativa de componentes de Big Data.

## **8. Interoperabilidad entre blockchains**

Las blockchains tienen una estructura interna que no permite la interoperabilidad nativa. Recurrir a las API (*Application Programming Interface*) es el único medio eficaz que permite a las distintas blockchains comunicarse entre ellas. Así se han creado algunos puentes que permiten hacer corresponder los números de cuenta y los activos entre dos blockchains.

El intercambio de criptomoneda es virtualmente posible, pero el intercambio de activos más complejos (p. ej.: un "chat" virtual) exige que el objeto "chat" y su definición estén programados de la misma manera entre las dos blockchains. Cuanto más complejos se hacen los objetos, más disminuye la probabilidad de poder hacer corresponder dos blockchains. Sin embargo, en vista de los últimos desarrollos, las blockchains genéricas como Ethereum van perdiendo poco a poco su sentido. En efecto, para alcanzar un nivel de velocidad de transacciones razonable, parece necesario optimizar el tipo de datos enviados y, por lo tanto, el tipo de objeto asociado a ellos.

El problema será todavía más apremiante con las blockchains permisionadas que permiten intercambiar objetos especialmente complejos. Ciertamente, será indispensable una coordinación entre las distintas tecnologías e iniciativas. Los fundadores de las principales tecnologías son conscientes de ello, y tienen participaciones cruzadas en los consejos de administración que las dirigen.

## **9. Ordenador cuántico**

El ordenador cuántico no es un mito. Su existencia es indudable, con muchas experiencias ya disponibles destinadas a fines comerciales. Su potencia todavía es completamente relativa y se limite a algunos cúbits. El punto fuerte de la herramienta reside especialmente en la oportunidad que ofrece. Los sistemas informático físicos actuales, especialmente en el ámbito de la inteligencia artificial, exigen una gran cantidad de cálculos que se leen, escriben y releen una gran cantidad de veces. En el conjunto de la operación de cálculo, más del 90 % del tiempo puede estar dedicado a leer y escribir datos. Con los sistemas cuánticos, estas etapas ya no son necesarias. Además, la potencia de cálculo es exponencial en cuanto a cantidad de cúbits.

Por eso, hay usos comerciales que ya están disponibles para aplicaciones muy específicas. IBM parece ser la empresa más avanzada en este tema.

Las blockchains, ya sean públicas o privadas, se basan en dispositivos de cifrado y el fundamento de estos dispositivos es la teoría de los números primos. Sin embargo, superar las claves de cifrado implica cálculos con una gran cantidad de lecturas y escrituras. El uso de ordenadores cuánticos reduce en gran medida el tiempo necesario para superar una clave. Así, la seguridad asociada a las tecnologías blockchain corre el riesgo de verse amenazada con la aparición de estas tecnologías.

Para protegerse, ya hay contramedidas en marcha. Hay muchos planteamientos de encriptado disponibles. Uno de las más conocidos reside en los algoritmos denominados post-cuánticos, entre los que figuran, por ejemplo, los algoritmos elípticos. En cambio, el uso de este tipo de algoritmos tiene un impacto negativo sobre el rendimiento técnico de blockchain. Por otro lado, se han implantado muy pocas soluciones con estas contramedidas.

La red Bitcoin ha tenido éxito muchas veces al cambiar la complejidad de su algoritmo de cifrado. Por lo tanto, el desafío es superable.

# Desafíos de la actividad

Algunas limitaciones están más vinculadas a los procedimientos y métodos de trabajo que a los aspectos técnicos. Los informáticos conocen bien este problema.

Las dificultades recurrentes que hay que prevenir en el futuro engloban los problemas de derecho al olvido, la gestión del error, la revisión de los procedimientos y de los métodos de trabajo así como los recursos humanos necesarios para el mantenimiento del nuevo sistema.

## **1. Derecho al olvido**

El derecho al olvido es un componente importante en los sistemas de información modernos.

En España, la Ley Orgánica 03/2018 de Protección de Datos Personales y garantía de los derechos digitales regula el uso y gestión de la información que contiene datos de carácter personal, y la Agencia Española de Protección de Datos (AEPD) es la encargada de velar por su cumplimiento. Los usuarios que lo deseen pueden solicitar la eliminación de datos a gigantes tecnológicos como Google o Facebook.

El problema se encuentra en blockchain. Por supuesto, es difícil encontrar una transacción sin ID, pero la información se guarda almacenada en la cadena para siempre. Por lo tanto, en principio no es posible «limpiar» la cadena de información concreta. Por ejemplo, los antecedentes penales de una persona condenada se eliminan después de varios años sin infringir la ley.

Si no es posible quitar un dato, en cambio es posible utilizar la particularidad de los árboles de Merkel en algunas cadenas. En efecto, los árboles de Merkel tienen la propiedad de poder actualizar una información sin eliminar todo su contenido. Así es posible ver evolucionar con el tiempo a una persona o a un objeto. Se trata de la única alternativa posible en la actualidad, aunque no está extendida a todas las blockchains.

Ya hemos mencionado el problema en este libro.

## **2. Gestión del error**

En el estado actual de los métodos de trabajo, antes de realizar una transacción de manera efectiva se realizan muchas verificaciones. Aquí hablamos de transacción en el sentido general del término. Así, el concepto de transacción engloba las etapas desde el diseño hasta la entrega del producto.

Solo nos queda saber en qué etapa exacta queremos insertar una información en una blockchain. Durante las transacciones rutinarias, es necesario insertar la información en el sistema inmediatamente para que la transacción sea validada lo más rápido posible, sin tener que recurrir a un tercero de confianza. Durante las transacciones más comprometidas o complejas, parece necesario añadir procesos de control adicionales antes de proceder al registro.

Desde un punto de vista teórico, los smart contracts que se encuentran en una blockchain dada pueden ocuparse de estos controles. Conceptualmente, estos controles existen en los métodos de trabajo actuales. Sin embargo, los sistemas de información utilizados hoy en día en la banca o en la industria, a menudo son muy permisivos. Este aspecto permite una flexibilidad real del sistema frente a un entorno cambiante. Por eso, hombres y mujeres realizan una parte importante de los controles.

En el marco de los smart contracts, este control se realiza a nivel de la aplicación descentralizada y de los contratos. Si la permisividad de estas pruebas está mal adaptada, puede estar seguro de que las dificultades operativas se acumularán con rapidez. Entonces parece poco probable a corto plazo que esté en peligro el empleo de las personas encargadas de controlar el pre-registro en una Blockchain o en una base de datos.

Es acertado dejar estos controles en manos de humanos para protegerse contra un bloqueo total en la cadena de operaciones porque el sistema de información no está programado. El humano también permite limitar los errores, porque todos los controles no están forzosamente diseñados, programados y presupuestados. Entonces, el humano es el botiquín de primeros auxilios en muchas situaciones. El personal de los back-office y de administración a veces dedica a estos controles hasta el 80 % de su actividad.

## **3. Una reestructuración de los procedimientos, de los métodos de trabajo y de las mentalidades**

Blockchain se ha convertido en una tecnología nueva que puede venir a completar el arsenal de las tecnologías existentes. A cambio, viene a alterar en gran medida la organización de la dirección del proyecto y de los métodos de trabajo en las empresas.

A un técnico le cuesta varios días poner en marcha un prototipo para comprender cómo funciona la tecnología. En cambio, cuando se trata de iniciar un proyecto auténtico, el conjunto del proceso cambia, con una cantidad de intervinientes muy elevada.

Para empezar, es posible que las organizaciones clásicas de proyecto no funcionen. En el marco de proyectos digitales clásicos, un departamento formaliza sus necesidades y monta un equipo compuesto por miembros técnicos y profesionales en una misma organización, y empieza a trabajar. Big Data ha demostrado las debilidades de este modelo vertical, porque lo fundamental del valor constatado se encuentra en el cruce de los datos (p. ej.: marketing con fabricación). Una fusión de este tipo no está prohibida por naturaleza, pero ha hecho que los colaboradores, que han visto disminuir su poder local, piensen de otra manera. En efecto, el que conocía y dominaba la información tenía un cierto poder.

En un contexto de blockchain, la constatación se realiza una vez más. Sin embargo, no se produce una desposesión de los datos en favor de un sistema nuevo. Al contrario, hay un enriquecimiento de los datos para facilitar el día a día de los operativos. Para poner un ejemplo, un caso de uso abordado por la tecnología tiene lugar en la gestión de los contratos y el pago de derechos de autor asociados a una actividad. La tarea de recogida de información y verificación cruzada es complicada, laboriosa y manual. Con blockchain, esto se reduce a unos segundos, aumentando de este modo la reactividad y el rendimiento de los equipos. Se utiliza mucho menos tiempo para coordinar la información y las personas. Este enriquecimiento frente a tareas conocidas por ser menos interesantes a los ojos de los operativos hace que la tecnología sea atractiva. En contrapartida, los especialistas pueden utilizar el tiempo liberado en beneficio de su actividad principal.

Respecto a los servicios informáticos, en cambio, se puede observar una crispación. A menudo, la tecnología es desconocida para ellos. Entonces es difícil posicionarse por una tecnología en particular. Incluso si se posicionan, muchas empresas la han elegido, su voz no tiene tanto peso como en el pasado. Hasta se les retira la posición de cliente proveedor en beneficio de un planteamiento colaborativo. La captación, a veces en bruto, de información desde su sistema hacia un datalake ha decepcionado a algunos. Los casos de uso a los que se han enfrentado pueden, una vez más, sencillamente cuestionar su estrategia digital. Las aplicaciones utilizadas o presupuestadas se transformarán inevitablemente, porque blockchain tiende a ser utilizada como una capa por encima de sus sistemas. Es posible que algunos teman perder el contacto con su usuario base cuando la tecnología acabe con las estructuras verticales y las canalice hacia una plataforma nueva.

Ya sea para el profesional o la informática, hay que encontrar nuevos métodos de trabajo y de organización. Las organizaciones verticales clásicas se enfrentan a una prueba dura. El planteamiento es fundamentalmente transversal, encontrar un presupuesto en una unidad en concreto tiende a perder su sentido. El Project Manager había perdido su poder en favor del Product Owner con el método Agile. Sin embargo, vamos a observar una serie de Product Owners repartidos en muchas empresas sin ningún responsable final. Eso implica mentalidades nuevas, incluso en los equipos, que deben admitir una pérdida de control en beneficio de un rendimiento colaborativo mayor. Hasta los equipos están fragmentados en varias ubicaciones, con grados de conocimiento y de competencia muy variados repartidos en procesos y sistemas distintos. El proceso de convergencia y la creación de los equipos exigen implantar métodos y gobernanzas draconianos.

Más que nunca, la gobernanza es clave. Hay que diseñar las normas de manera conjunta con los socios. La experiencia demuestra que tener un solo y único punto de contacto que aporta la posición de una empresa es el camino más seguro hacia el éxito. Los equipos con un miembro profesional y dos técnicos, por ejemplo, llevan inevitablemente a retrasos importantes de la organización. Esto implica una delegación de autoridad y una estrategia blockchain en cada grupo.

La gobernanza profesional transforma la lógica cliente proveedor en socio. Este planteamiento es la vanguardia de la industria alemana y un pilar de su competitividad en el mundo. Cualquier industria española que quisiera utilizar el pretexto de la tecnología para transformar las mentalidades y los usos, haría un servicio a su empresa mucho más importante de lo que cree y mucho más.

La gobernanza técnica es la aplicación de las necesidades de la actividad con la aplicación de los límites y de las buenas prácticas. Muchas veces se ha observado una falta de sincronización entre la experiencia y la técnica con la aparición de los procesos Agile. La interacción con otros miembros de equipos procedentes de otras empresas hace que el proceso colaborativo coordinado sea todavía más complejo.

En cualquier instancia, las tomas de posición dogmáticas prometen debates acalorados. Además de estos elementos, se necesita una formación adicional específica para las personas interconectadas. El trabajo es similar al de las asociaciones y exige dominar los métodos de trabajo colaborativo, especialmente los límites legales, antimonopolio por ejemplo, y un formalismo particular.

Por último, en el conjunto de la empresa, la ola blockchain va a imponer un cambio lento y progresivo de los comportamientos. Muchas industrias han iniciado campañas de formación de varios millones de euros para cambiar las mentalidades de los colaboradores. Estos cambios valientes no tendrán necesariamente un impacto a corto plazo en el rendimiento de la empresa en revisión. Sin embargo, esto creará el caldo de cultivo necesario para enfrentarse a los choques que impactan en las empresas cada dos o tres años.

## **4. Recursos humanos**

Los recursos humanos representan un auténtico freno a la aceptación de esta nueva tecnología y de la lógica que la sostiene.

El primer freno procede de la contratación. La tecnología es nueva, mal comprendida y está en pleno desarrollo. A menudo, la distinción entre cadena pública y cadena privada es poco conocida, y la dificultad técnica es alta. Encontrar el personal adaptado a estas nuevas tecnologías es complejo y laborioso.

Es tentador pensar en científicos y matemáticos especializados en criptografía. En la práctica, la tecnología está pensada para permitir su adopción progresiva por la mayor cantidad de personas. Especialistas reales trabajan para hacer que una comprensión de las claves privadas/públicas y de la manera de utilizarlas sea suficiente para hablar correctamente. Son útiles pero no son forzosamente necesarios para un equipo en un proyecto nuevo.

En sensato pensar en desarrolladores para hacer las aplicaciones en una cadena. Los lenguajes utilizados actualmente para desarrollar aplicaciones descentralizadas (p. ej.: Solidity, Go) son raros y los perfiles tienden a dirigirse hacia proyectos y tecnologías más convencionales. Es necesaria una fase de aprendizaje, pero la proximidad de los conceptos es suficiente para apropiarse de estos lenguajes todavía en fase de creación.

El tiempo de adquisición es comparable al aprendizaje de un framework nuevo como AngularJS.

Es importante mencionar la dimensión experiencia. Hay dos escuelas enfrentadas. La primera consiste en creer que una persona que conoce bien el trabajo debe dar soporte a la puesta en marcha del proyecto. La lógica espera que, como la persona conoce bien los procesos, la integración de una tecnología nueva será más fácil. El segundo planteamiento consiste en tomar una persona que no tenga tanta experiencia. Se utiliza su espíritu crítico y su capacidad de innovación para rehacer los procedimientos actuales. Entonces se buscan cualidades diplomáticas y de firmeza. En los dos casos, los responsables necesitan tener una comprensión real de la tecnología, para limitar los tropiezos.

Resumiendo, aunque hay varios límites, como el derecho al olvido, la gestión del error y la revisión de procesos, que son un freno para la implantación de la tecnología, el hombre es el que paradójicamente parece ser el verdadero freno a la implantación de cualquier tecnología nueva.

## **5. Multiplicidad de los tokens y gestión de riesgos**

Los años 2017 y 2018 fueron testigos de una explosión de criptomonedas, tanto en su variedad como en el tamaño de las inversiones realizadas. Algunas empresas y algunos gobiernos se lanzaron a la aventura de las criptomonedas.

Su uso presenta numerosos desafíos, la mayor parte muy conocidos por los gestores de fondos y de tesorería.

La diversidad de las criptomonedas hace que la gestión sea tan compleja como la gestión de las divisas en los mercados internacionales. Su variación está estrechamente relacionada entre ellas. Algunas excepciones salen del lote de su modelo económico. En este caso podemos citar el token *Binance*. La gestión de la volatilidad de las monedas y por lo tanto del riesgo que presenta es casi imposible con los instrumentos financieros clásicos. Las variaciones diarias son del 5 al 10 % mientras que los mercados financieros de acciones difícilmente evolucionan por encima del 1 %. Hay productos derivados que intentan emerger, especialmente en las bolsas de Chicago (CBOT), pero las iniciativas se rechazan con regularidad. Básicamente, los argumentos son la protección de los actores y la estabilización de las instituciones.

Su uso tendería a reducir las variaciones de cotización, de manera similar a su introducción en las materias primas a principios del siglo pasado.

Hay una posible solución: las stablecoins. Recordemos que hay tres métodos para estabilizar una divisa: garantía fiat, colateralizadas y no colateralizadas. La stablecoin es una innovación técnica y funcional que ha llevado a sus fundadores a creer que blockchain y la criptomoneda habían encontrado un nuevo impulso. En la práctica, no salió nada concluyente. Los auténticos problemas más bien parecen ser legales y de ecosistemas que ya utilizan los sistemas de monedas fiat que de volatilidad de las cotizaciones. Otro argumento: estos tokens no están, para la gran mayoría de ellos, respaldados por un contravalor en el mundo real.

Otro desafío sustenta la multiplicidad de los tokens: su intercambio. En las más de 2400 criptomonedas listadas hasta ahora, en 20 000 mercados distintos, los índices de cambio se consideran notablemente más altos que en los mercados tradicionales para intercambiar acciones de empresas.

Sin embargo, esta crítica oculta una verdad más alarmante. Para un profesional, los gastos de cambio son del 1 al 2 %. Para un particular, los gastos aumentan fácilmente hasta el 8 %. Este índice también se confirma para las transferencias en las plataformas de criptomonedas. Por lo tanto, la especulación es especialmente importante en algunas divisas.

Sin embargo, sería inexacto definir las inversiones masivas en la tecnología como realizadas exclusivamente con fines especulativos. En las primeras 100 capitalizaciones de blockchains disponibles, ninguna es inferior a 50 millones de dólares. Algo inimaginable dos años antes, donde la mayor parte de las capitalizaciones oscilaba alrededor de los dos millones de dólares.

# Desafíos legales

Quizás se trata de los desafíos más importantes a los que se ha enfrentado la tecnología. El Banco de España actual procede del Banco Nacional de San Carlos fundado por Carlos III en 1782. La Fábrica Nacional de Moneda y Timbre ha sido la única entidad acreditada en España para acuñar moneda desde que la peseta se convirtió en la moneda nacional. Psicológicamente, para las élites del país va a ser difícil aceptar el concepto de descentralización de generación de monedas.

Además, aceptar el concepto de criptomoneda es problemático para las fuerza gubernamentales. En principio, esto va contra sus intereses económicos. Montenegro, por ejemplo, no tiene moneda nacional. La moneda mexicana o de algunos países de Latinoamérica está tan devaluada, que han decidido abandonar la gestión de su moneda estatal. En los dos casos, estos estados han perdido el volante de la gestión económica y dependen de las elecciones económicas de Europa o de los Estados Unidos.

El problema no es insuperable. Los estados europeos han encajado el paso de la descentralización al aceptar formar un Banco central europeo.

El segundo problema trata sobre la idea de contrato. La Unión Europea ha señalado a España algunas profesiones que habría que desregular, especialmente la de notario. La tecnología Blockchain 2.0 puede transformar estas profesiones, es decir, provocar su desaparición tal y como se ejercen en la actualidad.

Sin embargo, es necesario que el estado que acepte esta tecnología reconozca que los smart contracts tienen el estatus de prueba en el marco legal, o de principio de prueba como mínimo.

Una vez más, el problema no es necesariamente insuperable. Históricamente, un estado legisla sobre toda práctica nueva o tecnología nueva con un retraso mayor o menor. Por otro lado, algunos proyectos (p. ej.: Corda) buscan conceder la propiedad ricardiana a los smart contracts.

El tercer problema reside en la retención de los impuestos sobre los bienes intercambiados por el intermediario de una criptomoneda. Se habla de un sistema descentralizado, encriptado y utilizando pseudónimos para identificar a los actores. Actualmente, los contables y notarios trasladan al estado las transferencias de bienes, así como el tipo de bienes. En función de las características de la transferencia, un bien de consumo corriente puede estar sujeto a impuestos bajo el concepto de "Impuesto sobre la Renta de las Personas Físicas (IRPF)" o "Impuesto de sociedades" o "Impuesto sobre el Valor Añadido (IVA)" u otros.

Si la tecnología se democratiza, ¿cómo establecer y trasladar a las autoridades estas transferencias? La pregunta todavía no tiene respuesta.

El cuarto problema reside en el estatus fiscal de la misma criptomoneda. A priori se trataría de un medio de pago. Pero todos los países no le han garantizado el mismo estatus a la criptomoneda más extendida: el bitcoin. El Reino Unido considera que el bitcoin es una moneda de intercambio, y por lo tanto no está sujeta a IVA. Australia concluyó que no se trataba de una moneda, porque el país definió que es necesario que una moneda sea emitida por un estado o una entidad gubernamental que actúa como tal. Por lo tanto, la criptomoneda está sujeta a IVA o GST (*Goods and Services Tax*, Impuesto sobre bienes y servicios). En los Estados Unidos, el bitcoin no está considerado como una moneda de intercambio, sino como un instrumento financiero o una propiedad, y por lo tanto está sujeto a impuestos sobre la plusvalía de las transacciones (Hern, 2014). Sin embargo, el FinCEN (*Financial Crime Enforcement Network*, Control de delitos financieros), los reguladores bancarios, la SEC (*Security and Exchange Commission*, Comisión de bolsa y valores), la CFPB (*Consumer Financial Protection Bureau*, Oficina de protección financiera del consumidor), la CFTC (*Commodity Futures Trading Commission*, Comisión de negociación de futuros de productos básicos) y el DOJ (*Department of Justice*, Departamento de justicia) consideran al bitcoin como una moneda.

Los recientes ajustes de 2018 confirman estas posiciones, y exigen que todas las criptomonedas inicien procedimientos ante la SEC, con muy pocas excepciones.

Francia desea ser uno de los primeros países europeos en legislar. Se han lanzado varias iniciativas legales con la entrega de un informe sobre blockchain a la Asamblea nacional en diciembre de 2018, seguido de la ley Pacte el 22 de mayo de 2019. Se han iniciado grupos de trabajo a nivel nacional donde se espera la futura integración de industriales.

Las iniciativas concertadas a nivel europeo están en pañales, pero existen. Las más avanzadas parecen proceder de la iniciativa ciudadana, especialmente con INATBA (*International Association of Trusted Blockchain Applications*, Asociación internacional de aplicaciones de blockchain de confianza) a la cabeza.

En España, el Ministerio de Hacienda publicó a principios de 2018 sus directrices para la declaración tributaria de criptomonedas, se pueden consultar en el Plan de Actuación de Control Tributario y Aduanero. En la práctica, las monedas virtuales no están sujetas a IVA, pero si hemos realizado una venta, las ganancias deben tributar como rentas sujetas a IRPF en el apartado "Otras ganancias patrimoniales". Los propietarios de criptomonedas deben informar a Hacienda de cuántas tienen y las operaciones que realizan con ellas. Para ello deben rellenar el modelo Declaración informativa sobre bienes y derechos situados en el extranjero. Las criptomonedas se consideran activo intangible y solo tributan cuando se convierten en dinero fiat.

Esta posición no se opone totalmente a las ventajas de blockchain, de la criptomoneda y del protocolo entre pares. Solo se controlan las plataformas de intercambio. Nada prohíbe intercambiar tokens o criptomonedas entre individuos, salvo la plataforma de intercambio profesional. Además, parece que la motivación de la ley obedece a una lucha contra el blanqueo de dinero y los abusos asociados.

En general, puede consultar la situación legal del bitcoin en el sitio dedicado: <https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country>. Al tratarse de un sitio comunitario, siempre debe verificar la información en los sitios oficiales de legislación financiera.

Por último, es importante recordar que existe una diferencia entre la ley y la aplicación de la ley. Teniendo en cuenta el aspecto global de la tecnología, parecería adecuado adoptar un planteamiento global de la legislación. Sin embargo, la tecnología Blockchain se distingue por su capacidad de ser transnacional. Más concretamente, los contactos asociados a una aplicación se pueden realizar obedeciendo a legislaciones y normativas locales.

La pregunta que se plantea es: ¿Quién va a legalizarlo primero? La mayoría de las veces, otros países siguen la línea de algo que ya existe.

Sobre todo, no hay que olvidar que todo no se resuelve mediante un contrato. Un bloque siempre será la expresión de una necesidad, y un smart contract su realización en un universo electrónico.

# El desafío del código abierto

En el marco de las aplicaciones descentralizados, los componentes fundamentales son principalmente de código abierto. El objetivo es permitir a la comunidad de desarrolladores proporcionar soluciones optimizadas sobre problemáticas encontradas por una tecnología dada. Para ilustrar el concepto, Big Data es una rama de la informática que se desarrolla gracias a la comunidad de código abierto, sin el que la tecnología subyacente nunca habría visto la luz.

El problemas tiene dos orígenes. Por un lado, hay que establecer un consenso sobre el conjunto de las transacciones y aplicarlo a nivel global. Por otro lado, es necesario aportar mejoras iterativas a los protocolos y programas. Entonces, el desafío recae en las versiones desplegadas y su instanciación en la red. Los debates sobre algunos puntos estratégicos o técnicos pueden ser tan virulentos como en el parlamento de España.

En la teoría de juegos, el consenso no siempre prevalece sobre una elección arbitraria hecha por un único agente. El contexto y las hipótesis de base son la causa de ello. Bélgica estuvo sin gobierno durante 541 días por la ausencia de consenso, esto es una demostración de este caso (La Libre, 2014). De manera similar, en caso de conflicto grave (por ejemplo: en caso de una guerra), donde entra en juego el retraso asociado a una toma de decisión, el consenso no es favorable.

La tecnología Blockchain está en constante desarrollo y mejora, y evoluciona por consenso. Únicamente, los repetidos ataques y los escándalos que han marcado el camino del bitcoin dan fe de los desafíos económicos. El sistema no es infalible (consulte la sección Desafíos técnicos). En el futuro, es posible que se descubran situaciones que exigen una toma de decisión ágil. Desde ahora, este problema se ha planteado con el bitcoin, que se enfrenta a grandes limitaciones técnicas compartidas por un determinado número de criptomonedas.

Para responder a este problema, es probable que veamos surgir un organismo similar a la Open Source Initiative. Entonces, el objetivo sería evitar situaciones imposibles de desenredar o «forks» tecnológicos que pudieran poner en peligro la estabilidad del sistema.

Un «fork» es una palabra inglesa que designa a una copia de un programa donde las características y funcionalidades se han alejado en un momento dado en el tiempo. Los creadores del triunvirato Blockchain, criptomoneda, protocolo par a par han contado con la improbabilidad de una divergencia evidente. En caso contrario, el comercio entre criptomonedas estaría muy comprometido, y la industria se enfrentaría a una escisión. Estos casos han sucedido con mucha frecuencia en la historia de la humanidad.

Por otra parte, se puede confiar en el efecto de posición dominante de ciertos actores o monedas para imponer determinadas elecciones técnicas, tecnológicas o estratégicas, como lo explica la ley de Murphy.

Para ilustrar este punto, en 1992, los especuladores, entre ellos George Soros, consiguieron hacer quebrar al Banco de Inglaterra, el equivalente al Banco de España, y acumular enormes beneficios. Su tamaño y posición eran claramente desfavorables frente a la fuerza de un organismo estatal.

No obstante, si el sistema de Blockchain ha resultado viable y fiable a gran escala, y cede bajo la presión de ataques y de consensos fallidos, no solo están en peligro algunos inversores o un país, como cuando se hunde una moneda tras una crisis financiera. La naturaleza de esta tecnología es internacional. Cuando se derrumbó el bloque soviético a finales de los años 90, se desplomaron las bolsas de todo el mundo, y muchos miles de millones de dólares de PIB se evaporaron debido a la falta de pago de las deudas contraídas por los países de la antigua URSS.

# El problema de los forks y el problema más general de las versiones

Hace mucho tiempo que la empresa Oracle y la tecnología Java conocen este problema. ¿Cómo se puede estar seguro de hacer funcionar esta tecnología en entornos de trabajo muy distintos (p. ej.: UNIX, Windows, iOS)? ¿Cómo asegurarse de que todos los usuarios de la tecnología disponen de la misma versión? Oracle decidió utilizar una máquina virtual. Apple, por su parte, instala actualizaciones predeterminadas en iOS. Ethereum ha hecho la misma elección al crear máquinas virtuales. Una máquina virtual es un entorno informático emulado en un terminal (smartphone, ordenador, etc.). La máquina permite la ejecución de un programa en un sistema operativo donde no se habría podido ejecutar de otras manera. De manera similar, es como crear una embajada en un país extranjero. Mientras estamos en un país extranjero, el idioma y las leyes del estado representado se aplican en el recinto de la embajada.

El planteamiento más sencillo consiste en exigir a los usuarios que actualicen sistemáticamente la versión de uso de la base. Sin embargo, esta idea todavía no ha conseguido el consenso. El motivo está relacionado con los problemas técnicos que pueden encontrar las aplicaciones que utilizan esta base para funcionar.

## **1. Estudio de caso: TheDAO**

El problema de los forks se ilustró escandalosamente en julio de 2016 con TheDAO. TheDAO es una DAO, es decir, una organización autónoma descentralizada, fundada por los creadores de Slock.it. Recordemos que una DAO funciona como se describe a continuación.

Un grupo de programadores escribe smart contracts (programas) que tienen la misión de hacer funcionar la organización.

Un período de 28 días permite recaudar fondos para donar los recursos necesarios al funcionamiento de la organización. A cambio, la DAO distribuirá tokens, o criptomonedas, a los inversores afectados.

Es importante destacar que estos tokens no dan ningún derecho de propiedad: solamente dan un derecho de voto. Eso se llama una ICO (*Initial Crowdfunding Offering*), de manera similar a una IPO (*Initial Public Offering*) en finanzas.

Al final de período de recogida de fondos, la DAO podrá funcionar.

Entonces, los participantes en la DAO tienen la capacidad de proponer proyectos para utilizar mejor los recursos invertidos. Los inversores, por su lado, disponen del derecho a voto en función de la cantidad invertida.

Por definición, ninguna DAO es propiedad de nadie. De hecho, los programas que la hacen funcionar son los que hacen la ley.

TheDAO es el nombre de una DAO específica fundada el 30 de abril de 2016 por un equipo alemán, Slock.it, conocido por los smart locks. Se trata de contratos pequeños que permiten el alquiler de bienes, como casas o coches, de manera similar a Airbnb, pero de manera descentralizada.

El 15 de mayo, las inversiones en TheDAO superaron los 100 millones de dólares. Al terminar el período de recogida de fondos, las cantidades recogidas superaron los 150 millones de dólares, recogidos entre más de 11 000 inversores. Este entusiasmo superó con creces toda esperanza, porque eso representaba casi el 15 % de los ethers disponibles en la plataforma.

Sin embargo, TheDAO, al contrario que el protocolo Ethereum, era conocido por tener algunos errores, especialmente cuando el 12 de junio de 2016, Stephan Tual detectó un error de llamada recurrente. Una función se llamaba varias veces por error.

Es importante destacar que la fundación que da soporte al protocolo Ethereum, actualmente no lamenta ningún error conocido. De manera similar al protocolo Bitcoin, el protocolo Ethereum no padece ningún problema que ponga al sistema en peligro. Desde que existe el protocolo Ethereum, ningún ataque ha podido poner en peligro la plataforma, que ya representa aproximadamente mil millones de euros en los smart contracts desplegados actualmente.

### a. El ataque

Al terminar la recogida de fondos, había unos cincuenta proyectos en estudio. El equipo de TheDAO solucionó algunos errores de funcionamiento de la DAO, cuando detectó que los fondos recogidos eran transvasados de manera sistemática por una tercer entidad. La información se hizo pública inmediatamente. Habían robado la considerable suma de 3,6 millones de ethers, es decir, aproximadamente 50 millones de euros.

El 17 de junio, la cotización del ether pasó de alrededor de 18 euros por ether a 11 euros por ether en un solo día.

El procedimiento de ataque era bastante sencillo. La persona, o el grupo, al origen del ataque crearon una DAO hija, completamente idéntica a TheDAO, primero utilizaron un bucle recursivo para captar los fondos, como si se tratara de un proyecto votado por los inversores, y por lo tanto apropiado para estos fondos. Sin embargo, esta captación de fondos seguía las reglas de TheDAO. Eso implicaba que estos fondos debían permanecer bloqueados durante 28 días antes de poder volver a transferirlos a la economía real.

### b. Soluciones propuestas

Técnicamente, es posible saber a qué dirección están asociados los fondos captados. Sin embargo, no es posible saber exactamente la identidad de la persona antes de que los transfiera a una cuenta bancaria.

La idea propuesta por el equipo original del proyecto para limitar las pérdidas era escindir TheDAO en dos. El problema: era imposible reunir bastantes votos en tan poco tiempo.

Después de varios días se propusieron dos soluciones: un soft fork y un hard fork.

La primera solución consistía en no tocar el bloque que comprendía la transacción de los 50 millones usurpados. Sino invalidar toda llamada a la dirección que había captado ese dinero. En pocas palabras, eso significaba que los 50 millones desaparecerían de la economía en la plataforma Ethereum, y también de la economía real, porque ese dinero, que entonces estaba en ethers, originalmente estaba en dólares, euros, etc.

Si se tomaba una decisión como esta, había que implementarla antes de 27 días, porque después los fondos ya no podrían recuperarse completamente. En efecto, la DAO hija podría haberlos utilizado una vez pasado el período de incubación de 28 días.

La segunda solución consistía en anular la transacción, lisa y llanamente. Todo el dinero depositado en la estructura de los contratos empleados por TheDAO es recuperable en dinero real (dólares, euros, etc.). Eso implicaba que incluso las entidades hijas de TheDAO podían ver transvasados sus fondos, con ayuda de una función creada para la ocasión. Al terminar la recuperación de los fondos, TheDAO moriría y cerraría sus puertas.

### c. Problemas asociados a estas soluciones

Para cualquiera de las dos soluciones se presentaban muchas dificultades.

En primer lugar, parecería que el atacante había emitido una carta abierta para protegerse contra las dos soluciones contempladas. Utilizamos el condicional porque, en principio, la firma que aparecería en la carta abierta sería falsa.

En la carta, el atacante advertía de que el método empleado para transvasar los fondos era perfectamente legal, y que utilizaría todos los medios legales a su disposición para defender su propiedad. ¿Realmente era necesario? El dinero extraído le concedía un derecho de voto importante. Además, estaría sometidos a los correspondientes impuestos, porque tendría que declarar beneficios según su país de origen. Los gastos legales también serían astronómicos, teniendo en cuenta que TheDAO está en una zona gris desde el punto de vista legal.

Los fondos proceden de varios países, donde la política fiscal e incluso la aceptación de la moneda virtual no siempre existen jurídicamente.

El atacante completaba su estrategia del palo con la zanahoria. Si la comunidad favorecía el minado de la moneda que había robado, el pirata recibiría una gratificación de 1 millón de ethers (además de los 3,6 que faltaban) junto con 100 bitcoins.

Además, si los fondos tenían que ser recuperados por los poseedores de derechos iniciales, el atacante podría, según las legislaciones, pedir los fondos a cada inversor y no a TheDAO. En términos jurídicos, esto se llama una operación de Pascal. Peor, el ataque podría pedir más que los fondos introducidos, por los daños sufridos, por ejemplo.

Problema adicional: algunas entidades empezaron a realizar intercambios tomando como base los contratos propuestos por TheDAO y la versión 1.0 de su código. Este planteamiento implicaba que las empresas y contratos terceros que utilizaban estos contratos estaban sujetos a esta inversión de flujo.

Entonces, los inversores iniciales de TheDAO podrían recuperar más dinero que los fondos invertidos inicialmente. Las plataformas de intercambio no estarían excluidas. Los mineros, que invalidarían la transacción, y así escribirían la versión «deseada» en lugar de la versión «real», también podrían ser potencialmente perseguidos, como si hubieran dado falso testimonio.

Problema complementario: por definición, una DAO funciona sin intervención humana. Fuera cual fuera la solución adoptada, se opondría a la filosofía de las aplicaciones descentralizadas. Muchos observadores estaban de acuerdo en que no hacer nada era peor que dejar que el dinero invertido se fuera. Había una gran cantidad de paralelismos con el sector financiero y sus decepciones de los diez últimos años para justificar una intervención o no en la nueva captura de este dinero.

### d. Solución final

La solución final elegida fue la del hard fork. Entonces se reembolsaría a los inversores hasta el último céntimo. También se constató la creación de una duplicación de moneda con unas siglas nuevas. En lugar de ETH que se conservó para el hard fork, se adoptó ETC, por Ethereum Classic: la rama difunta.

A pesar de todo, la posición del pirata estaba valorada en 6 millones de euros en la cadena antigua. Muchos especialistas invitaron a los mineros puristas a cambiar a la nueva. Más que una cuestión de filosofía, era un proceso sólido y duradero que necesitaba a la tecnología para alcanzar su pleno potencial. ¿Quién se preocupa hoy en día por tener un lector de DVD Blu-ray o HD?

De todo esto se pueden extraer algunas normas de sentido común para el futuro. Los creadores de TheDAO no esperaban tanto entusiasmo. Por eso habían colocado todos los fondos en una sola cuenta, una sola dirección. El equipo de Ethereum y el de TheDAO invitaron encarecidamente a los iniciadores de proyectos a no colocar más de 10 millones de euros equivalentes en una cuenta, para limitar futuros sinsabores.

La tecnología todavía está dando sus primeros pasos. Por lo tanto, es muy probable que se tomen este tipo de decisiones de manera excepcional. Los forks son perjudiciales de manera sistemática, sobre todo si dividen por igual las partes tomadoras. Hay que observar este problema con mucha atención, sea cual sea su origen.

# Desafíos de la volatilidad de las criptomonedas

En agosto de 2019, el bitcoin estaba valorado en aproximadamente 9377 euros (Investing, 2019). El 18 de julio de 2010, valía 0,0858 euro, es decir, unas 110 000 veces más en menos de diez años. La desviación típica, que permite medir la variación de la moneda, en este período fue de 3277,29. Por el contrario, si tomamos el índice de cambio entre el euro y el dólar, encontramos una desviación típica de 0,04.

Estos dos datos permiten cuantificar el rendimiento de una moneda y el riesgo asociado a este rendimiento. En el sector financiero, es una práctica habitual cuantificar el rendimiento de una posición y dividirlo por su desviación típica. El bitcoin alcanzó una relación cien veces mejor que el dólar para una inversión en euros. De lo que se deduce que, a priori, invertir en el bitcoin es increíblemente más rentable que invertir en dólares.

La siguiente figura representa la variación del euro frente al bitcoin y la variación de la cotización del euro frente al dólar.

Escala de tiempo

Descripción generada automáticamente

*Cotización del euro frente al dólar y cotización del euro frente al Bitcoin desde el 1 de mayo de 2015 hasta el 1 de agosto de 2019. Fuente: Investing.*

El gráfico presenta de manera bastante clara las variaciones significativas. La criptomoneda en cuestión evoluciona con picos mucho más pronunciados. Sin embargo, esta observación no se limita a una sola criptomoneda. La mayoría de las monedas digitales tienen el mismo problema, como Counterpartycoin, Litecoin, Percoin, Namecoin, Terracoin, Devcoin o Novacoin.

No obstante, en comparación con otras divisas digitales, el bitcoin muestra una volatilidad, cuantificada matemáticamente por la desviación típica, inferior a la de otras criptomonedas. Además, no todas las criptomonedas son minables (por ejemplo, Ripple o la difunta TheDAO). Sin embargo, la velocidad de minado de una criptomoneda parece influir de manera positiva en su volatilidad. El rendimiento no parece estar relacionado con la facilidad de minado.

A corto plazo se puede sacer una segunda constatación. El entusiasmo por la creación de criptomonedas nuevas es exponencial. En abril de 2013, se podía observar e invertir en siete criptomonedas. En agosto de 2019, encontramos 2400, es decir, en tres meses la cantidad de criptomonedas se había multiplicado más de doscientas veces (Coinmarletcap, 2019), con valores de mercado capitalizados que varían entre 1 millonésima de dólar y 9000 millones para el bitcoin. El segundo (Ethereum), en comparación solo representaba 1000 millones de dólares.

Así, es posible crear su propia criptomoneda a voluntad, solo algunas se utilizan con una capitalización consecuente. Se observa que la capitalización de los Altcoins está muy relacionada con la del bitcoin, que actualmente parece actuar como valor de referencia.

Gráfico, Gráfico circular

Descripción generada automáticamente

*Principales capitalizaciones de las criptomonedas cotizadas. Fuente: personal, basada en CoinMarketCap*

Estas observaciones ocasionan dificultades operativas importantes. En primer lugar, si queremos utilizar Bitcoin como medio de intercambio viable y fiable, la volatilidad de la cotización debe estar mucho más contenida.

Este es el criterio que permite a las cinco monedas más habituales del mundo servir como base de intercambio.

Paradójicamente, la segunda dificultad surge de la mente humana. Las ciencias sociales han demostrado que la mente humana funciona con sesgos de anclaje. Si una moneda evoluciona con rapidez, el cerebro humano puede crear estándares, llamados anclas, que no están necesariamente relacionados con la realidad técnica o económica.

Así, si una aplicación necesita más de 100 tokens de una criptomoneda dada para colocar en el campo STARTGAS (startgas es la cantidad de divisa necesaria para proceder a la operación de cálculo) para funcionar, el operador dispuesto a prestar su potencia de cálculo puede ser propenso a realizar la operación únicamente si se le remunera personalmente con 200 tokens para priorizar el cálculo.

De esta manera, los importes intercambiados pueden alcanzar picos sustanciales si la potencia de cálculo en una red dada es inferior a la demanda.

En teoría conductual y económica, una constatación establece que el bitcoin está sujeto a varias de cotización muy fuertes. Una persona que invierte en bitcoin asume riesgos desmesurados invirtiendo en el Bitcoin o en cualquier otra criptomoneda, en comparación con el euro o el dólar americano. Entonces debería esperar una prima de riesgo. Esta consideración se abstrae de los repetidos escándalos y robos en el mercado de los bitcoins desde su aparición.

Sin embargo, esta prima de riesgo se materializa en un grado de dificultad en el algoritmo de minado. Sin embargo, los dos mecanismos no funcionan de manera coordinada. El nivel de dificultad únicamente evoluciona en función del tiempo empleado en resolver un puzzle (proof-of-work). Este nivel de dificultad está programado de manera no modificable y evoluciona en función del tiempo empleado en resolver el puzzle del bloque anterior. El valor tiempo crítico está fijado en 10 minutos. Así, cuando más rápido se resuelve un puzle, más aumenta este grado de dificultad. Por naturaleza, la relación recíproca es cierta.

En teoría, cuantos más demandantes hay de una criptomoneda, y más grande es la cantidad de máquinas puestas a disposición por los mineros, estos últimos esperan obtener beneficios de la remuneración vinculada a la actividad de minado. En la práctica no es así.

Si la demanda de criptomoneda es exponencial, el aumento de la cantidad de máquinas listas para minar es lineal, porque está sujeto a limitaciones materiales. En conclusión, sin importar la cantidad de máquinas que minan, el tiempo de cálculo siempre oscilará en torno a los 10 minutos, a excepción de los Litecoins. Esta limitación de tiempo está sujeta a debate, pero representa un desafío con el que se encuentran todas las criptomonedas.

Lejos de estas consideraciones, se observa que cuando un mercado se organiza en torno a una plataforma de intercambio, la volatilidad de los productos intercambiados disminuye sustancialmente. Cuando el mercado está asociado a una plataforma de productos derivados, el efecto aumenta. Vamos a ver una demostración histórica, podemos observar el desarrollo del mercado de las opciones sobre materias primas en los Estados Unidos a finales de siglo XIX (Hull, 2006).

Así, si hubieran tenido plataformas de intercambio similares a CBOT (*Chicago Board of Trade*), hubiera sido posible ver emerger las ecuaciones y reducir la volatilidad de las ecuaciones, a pesar de la creación de criptomonedas nuevas. Este tipo de plataformas no existe todavía; en algunos países las soluciones existentes apenas pueden vivir de sus actividad.

También hay que destacar que aunque existen 178 monedas reconocidas internacionalmente en el mundo, solo 5 se intercambian con volúmenes significativos (más específicamente: el euro, el dólar americano, el franco suizo, el yen japonés y la libra esterlina). Esta observación podría hacerse en el ámbito de las criptomonedas. Habitualmente, se observan intercambios importantes en bitcoins, sustancialmente menos en divisas del protocolo Ethereum, etc.

El segundo factor que permitirá una disminución de la volatilidad está directamente relacionado con la cantidad de actores que utilizan esta tecnología. Cuantos más actores haya, más se acercará el valor de la criptomoneda a su valor auténtico, sencillamente mediante la aplicación del teorema de los grandes números. El problema para los profesionales consiste en saber cuál es el tamaño crítico del mercado a partir del cuál lanzar una plataforma de intercambio rentable.

Para el desarrollo de las aplicaciones descentralizadas, el problema sigue siendo el mismo, porque depende directamente del tamaño de la clientela de las plataformas de intercambio. En efecto, un actor está muy interesado en pasar por una plataforma para convertir su criptomoneda en otra divisa o criptomoneda.

Como las aplicaciones descentralizadas utilizan estos tokens, su carga aparece como directamente relacionada con las plataformas.

La única alternativa aparente es liberarse de estas criptomonedas públicas y crear nuestra propia criptomoneda en una empresa. En principio, estará menos sujeta a las variaciones del mercado, porque se trata de generarla internamente. Esta criptomoneda se utiliza en la empresa para realizar tareas dadas siguiendo un algoritmo. Por ejemplo, un robot puede verificar en cualquier momento que todos los clientes de un banco tienen su cuenta corriente en positivo, sin que haya un ojo humano para verificar el estado de las cuentas. Sin embargo, una operación de este tipo no tendría en cuenta la potencia de cálculo distribuida buscada por la red entre pares.

# Riesgos de mal uso de blockchain

Ya lo hemos visto, el funcionamiento de blockchain se regula automáticamente mediante el código y las reglas decretadas a través de los smart contracts. Sin embargo, el carácter descentralizado de la tecnología hace que sea muy difícil controlar todo lo que no está en blockchain y especialmente sus interfaces con el mundo exterior. Así, no es posible verificar la identidad del poseedor de una dirección Bitcoin, por ese motivo esta moneda se puede utilizar para comprar mercancías prohibidas o en circuitos financieros fraudulentos.

De esta manera, los terceros de confianza conservan toda su razón de ser como «guardianes de las puertas de blockchain». Para que esta tecnología se despliegue a gran escala, deben poder ser capaces de validar la entrada de nuevos participantes en el sistema, que por definición no puede ser validada por el mismo sistema. Todavía no se han inventado los medios para este control. Algo que muy probablemente pasará por el uso de blockchains híbridas o privadas con accesos reservados a los participantes acreditados, en contraste con las blockchains públicas como los bitcoins abiertos a todos.

Por otro lado, algunas empresas emergentes se posicionan en este segmento y se ofrecen para ayudar a los reguladores con su tarea analizando los flujos de transacción.