TECNOLOGÍA *BLOCKCHAIN*

LA REVOLUCIÓN DE LOS SISTEMAS CONTABLES

Dr. Basilio Ramírez Pascual

Por si no se han dado cuenta, el tiempo corre que es una barbaridad y estamos en 2019, es decir casi en el 2020 y según mi opinión estamos muy cerca de una revolución absoluta de lo que hoy entendemos por contabilidad por partida doble.

Blockchain o "Cadena de Bloques" es la tecnología que probablemente marcará en futuro de la contabilidad.

Por Basilio Ramírez Pascual
The Matrix Tributario

Índice

1 TECNOLOGÍA *BLOCKCHAIN* Y CONTABILIDAD

Como he indicado en la definición, la "cadena de bloques" es un libro de registro de datos: un libro de contabilidad digital de transacciones, acuerdos, contratos… **cualquier otra cosa que necesite ser registrada de manera independiente y verificada.**

La gran característica de este libro de contabilidad es que no se almacena en un solo sitio, sino que se distribuye a través de varios, cientos o incluso miles de computadoras de todo el mundo, dando acceso a cualquier persona de la red a una versión actualizada.

Los registros generales se amontonan en "bloques" y luego se unen criptográficamente y cronológicamente a una "cadena" que utiliza complejos algoritmos matemáticos.

Cada bloque recibe una firma digital única.

Una vez actualizado, el libro no se puede alterar ni cambiar, solo se pueden añadir cosas, y se actualiza para todo el mundo en la red al mismo tiempo.

La naturaleza distributiva de la base de datos de la cadena de bloques implica que es más difícil para los hackers atacarla: tendrían que acceder a cada una de las copias de la base de datos simultáneamente para tener éxito.

También mantiene los datos seguros y privados porque el resumen criptográfico no puede volver a convertirse en datos originales.

Esto quiere decir, que con independencia de si esto resulta más o menos comprensible para nosotros (los seres humanos más o menos inteligentes); lo que es un hecho es que lo que se escribe en **el libro contable Blockchain resulta inalterable, no podrá ser modificado, ni falsificado y quedará en un registro público por siempre jamás.**

Lo que significa, que si usted por ejemplo, envía una cantidad de dinero a un proveedor a través de estos sistemas, la transacción quedará grabada en una línea de este libro sin que pueda ser alterada y además podrá ser consultada por cualquier persona en el futuro, incluida la Agencia Tributaria.

¿Les suena esto de que en los libros contables no se puede tachar, ni raspar …? Es un texto común en los principios contables de las diferentes normas contables anteriores.

Un ejemplo básico de su aplicación en el mundo de la música:

La tecnología Blockchain sustituirá los formatos informáticos usados actualmente por uno nuevo bajo la denominación bc. cuyo contenido no sería únicamente la grabación fonográfica, sino también un enlace al registro Blockchain con información sobre esta grabación. El objetivo es **determinar automáticamente,** ante cualquier tipo de composición musical, **quién tiene los derechos de autor sobre la canción**, quién sobre el artista, quién sobre el intérprete y ejecutante y quién sobre la grabación.

Sin embargo, este no es un camino sencillo con objetivo cercano. La relación Blockchain con el mundo de la música tiene que enfrentarse a diferentes retos legales; habrá que explicar a las autoridades que este tratamiento está amparado por el interés legítimo del autor, y que corresponde a la necesidad de cumplir con la **obligación legal** de hacer valer los derechos morales y de paternidad sobre una canción.

Otros ejemplos que ya están aquí.

Los "Contratos Inteligentes":

Las monedas virtuales han traído importantes beneficios directa e indirectamente. La tecnología Blockchain ha acaparado la atenta mirada de muchos sectores, como ya hemos visto en las líneas anteriores. Empresas y consorcios que operan en el sector financiero han reajustado ciertos modelos que venían aplicando para adaptarse a los beneficios de Blockchain, consiguiendo una **importante reducción de costos económicos y temporales en las transacciones.**

El próximo paso son lo que se conoce como "Contratos Inteligentes" mediante los cuales se permite llevar a cabo negociaciones de una manera más segura y eficaz. Los "Contratos Inteligentes" consisten en un programa informático construido sobre unas reglas que permiten realizar un acuerdo quedando debidamente registrado. La esencia de este software son los algoritmos que, dada una condición determinada, automáticamente dará paso a otro proceso en el cual se transmitan los activos involucrados a la persona destinada. **La tecnología Blockchain permite registrar y monitorear perfectamente las transacciones de activos a través de la red**, garantizando que cada persona obtenga lo estipulado en el contrato de forma automatizada, una vez se cumplan las condiciones previamente establecidas.

El hecho de ser un proceso automático **elimina la participación de terceras personas**, aminorando el coste y tiempo extra de los que hablábamos al comienzo.

Los "Contratos Inteligentes" son un conjunto de archivos que contemplan unas determinadas órdenes. Éstos se ejecutan en un libro mayor descentralizado, donde se constituyen una serie de compromisos unilaterales que, si se cumplen las condiciones, proporcionaran una serie de activos.

Una vez se cumplen las condiciones del contrato, se ejecutan los códigos de operación alojados en el script y los activos involucrados en el proceso llegan a las partes interesadas.

Si bien, **aunque sea un sistema fiable, no es cien por cien seguro.** Por ejemplo, la plataforma Ethereum, en noviembre de 2016 presentó un fallo basado en la posibilidad de facilitar que los infractores alterasen la información, pudiendo sobrescribir otras variables allí inmersas que terminasen comprometiendo la integridad de los contratos inteligentes.

Los contratos inteligentes constituyen una herramienta de importante valor para el sector financiero, que, basada en la tecnología de las monedas digitales, están permitiendo acelerar las operaciones, dotándolas de mayor seguridad y efectividad, lo que hace pensar que le augura un exitoso futuro.

2 OTRAS APLICACIONES EN LAS QUE SE TRABAJA

Sistema de voto seguro

Actualmente, los sistemas de votación adolecen de una excesiva intervención humana, gasto en instalaciones, papeletas, personal... Un sistema descentralizado que reúna estas características sería muy útil en muchos ámbitos.

Y es que las máquinas electorales de recuento de votos se pueden trucar, se pueden registrar personas que no son ciudadanos, hacer ingeniería social y tratar que ancianos voten a favor de una determinada ideología…

Implementar el voto seguro parece una buena aplicación para incluir en la lista de las posibles a desarrollar con Bitcoin. A los participantes habría que proporcionarles una clave que les permitiría registrar su voto en la cadena de bloques, desde sus casas. Una vez que se haya votado, **los participantes podrían saber si su voto es tenido en cuenta o no** y en tiempo real se podría ir viendo el resultado de las elecciones a medida que los participantes vayan votando.

Este sistema ya ha sido utilizado en 2014. El partido danés Liberal Alliance, acudió a Bitcoin para llevar a cabo su proceso de votación interna de candidatos en 2014.

Registro documental

Si somos capaces de firmar un documento y fecharlo, si ahora ese documento lo introduzco en una cadena de bloques, estamos consiguiendo el resultado que perseguimos cuando acudimos a un notario. **El documento tiene fecha y no puede ser alterado**, porque la cadena de bloques no se puede alterar, a no ser que sea reconstruida desde el principio, algo que es muy difícil de hacer porque carecemos de poder computacional suficiente.

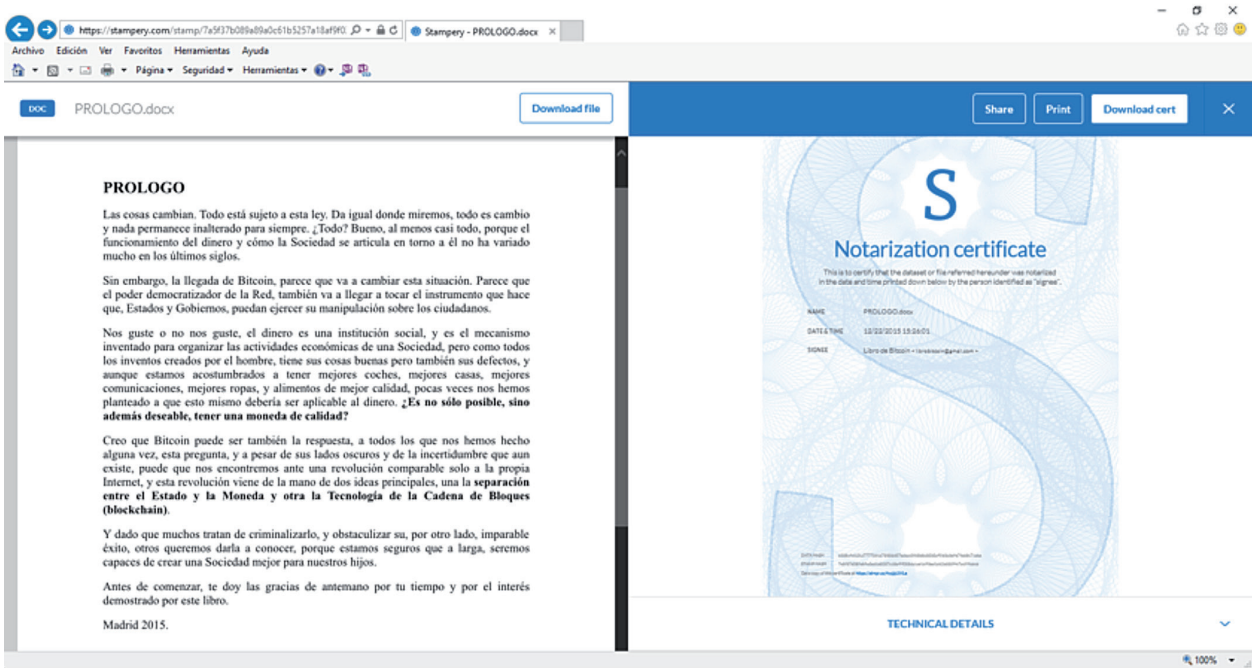
Además, jugamos con un factor muy importante de la cadena de bloques, y es que su registro es público. Esta técnica también podría utilizarse para registrar los títulos universitarios.

Otro avance curioso, pero avance, que podríamos conseguir mediante la cadena de bloques es, que, si conectamos un coche a la cadena de bloques, se podría registrar el kilometraje que hace, diciendo adiós a los trucajes que se hacen en los marcadores de kilómetros.

Ya hay varias empresas que proveen este servicio, algunas de ellas son:

- Stampery. – esta startup tiene varios españoles entre sus miembros. Permite la inclusión de documentos y correos dentro de la cadena de bloques proporcionando al usuario prueba de autoría, existencia e integridad con su solución.
- ProofOfExistence. - es un servicio que por 0,005 BTCs permite registrar en la cadena de bloques cualquier documento que indiquemos.

Y es que no hay mejor manera de ver lo que estamos diciendo que con un ejemplo:



"*Bitcoin, guía completa de la moneda del futuro*" por Santiago Márques Solís, es el libro en el que hemos basado la mayoría de este estudio. Este libro consta de un prólogo, el cual está registrado en la cadena de bloques. Aquí vemos un ejemplo realizado a través de Stampery.

Contratos digitales

Los contratos inteligentes o Smart contracts, se han puesto muy de moda con el impulso que están llevado a cabo el desarrollo de las criptomonedas. La idea de un contrato inteligente **podría introducir mejoras en los contratos legales tradicionales** que se escribían en papel.

Al igual que un contrato normal, un contrato inteligente es un acuerdo que se establece entre dos o más partes, pero tiene como condición que es capaz de ejecutarse y hacerse cumplir por sí mismo. Al ejecutarse sobre un entorno electrónico, no solamente las personas pueden beneficiarse de ellos, sino que es posible establecer acuerdos entre máquinas, lo que posibilita un abanico de aplicaciones dentro de otra área tecnológica.

Los contratos inteligentes **se escriben en un lenguaje de programación**, es un código que se ejecuta de manera automática siguiendo las reglas que se definen en su codificación. Y como las reglas informáticas son estrictas, no se necesita de intervención manual humana. Los contratos son capaces de interactuar en el entorno y conocer qué sucede para poder aplicar sus reglas a estas y devolver una conclusión.

Y ese entorno de interacción no es otro que la cadena de bloquees, y es dentro de Blockchain donde el contrato evoluciona, nace, se ejecuta y muere (si se da el caso).

Un ejemplo de hasta dónde puede llegar los contratos inteligentes sería: me compro un coche y tengo un préstamo asociado al pago del mismo, por tanto, he creado un contrato digital que está en la cadena de bloques. En caso de no hacer frente al pago de una cuota del préstamo podría revocarse el contrato, y si el coche estuviese conectado a internet, podría no dejarme arrancarlo. Y todo ello en tiempo real y sin necesidad de complejos procesos burocráticos que compliquen el proceso.

Para poder hacer esto posible, se necesita, al menos, los siguientes tres elementos:

1. Capacidades multifirma. – para la liberación de depósitos.
2. Dobles depósitos. – Eliminan la necesidad de un tercero de confianza mediante un algoritmo.
3. Los oráculos. - Posibilitan validar las cláusulas de un contrato que hacen referencia a condiciones externas de cualquier naturaleza y tipo. Solo si el acontecimiento externo se produce, la cláusula del contrato se valida.

Empresas como BitHalo, Stash, Blackhalo, Codius, Counterparty o RootStock, proveen servicios de contratos inteligentes, así como servicios adicionales.

El bufete de abogados londinense Selachiii, utiliza la tecnología de contratos digitales de Stash, y prevé para el próximo año ofrecer servicios de testamentos, registros de propiedad y acuerdos de accionistas.

Banco de Santander

El pasado 24 de agosto de 2016, elEconomista.com, se hacía eco de una noticia más que positiva para el futuro de la moneda digital.

Nada menos que el Banco Santander, junto con otras grandes entidades como el UBS, BNY, Mellon, Deutsche Bank, el operador de mercado ICAP y la startup Clearmatics, se han unido para **investigar y promover el uso del dinero digital entre instituciones financieras**, y como un primer resultado ha visto la luz una divisa similar a Bitcoin, la Utility Settlement Coin (USD), que permitirá la transaccionabilidad de activos reales sin necesidad de una gestión centralizada.

Este sistema tiene como objetivo facilitar pagos y liquidaciones de forma "*eficiente, rápida y segura*", mediante el uso de la tecnología Blockchain en la que se basan criptomonedas como Bitcoin "*para presentar y permitir la transaccionalidad de activos reales como euros o dólares*".

El coste para la industria financiera del sistema de compensación y liquidación de operaciones asciende a entre 65.000 y 80.000 millones de dólares anuales.

De este modo, USC sería una "moneda" que existe en un registro contable distribuido, es decir, en un Blockchain.

Las monedas digitales serían directamente convertibles en efectivo en los bancos centrales, **reduciendo el tiempo y el coste,** pero **aumentando la efectividad**.

"*El dinero digital será la clave en el futuro de los mercados financieros, y estará basado en el Blockchain, una tecnología que podría revolucionar la banca en los próximos años*" destaca el Banco Santander.

3 CONCLUSIONES

Como hemos visto la tecnología BLOCKCHAIN, asentada sobre la Red (internet) permite que todas las transacciones se realicen de manera totalmente trasparente, segura, independiente (sin intermediarios), inalterable por el fraude o la falsificación y sin autoridad central. **Es el Notario interactivo perfecto.**

Para los que hemos "trasteado" con las criptomonedas, es increíble ver lo sencillo que resulta enviar fondos a otro usuario en la otra punta del mundo y dar seguimiento a la transacción con tan solo un teléfono móvil. Y consultar la contabilización de ese envío en cualquier momento en un **Registro Público de la Cadena de bloques.**

Esto hace que, en el mundo, haya una gran actividad revolucionando lo que, hasta hoy, hemos entendido como contabilidad, AUDITORES (KPMG, Deloitte, EY y PwC, entre otros); Cadenas de Suministro, Sector Bancario, Consorcios, Registros Médicos, Registros de la Propiedad, Sistemas de Votación, Sistemas educativos globales ya estén utilizando esta tecnología, en la actualidad.

Ya están en marcha **contratos interactivos inteligentes** que por ejemplo no permiten el uso de un vehículo si no está al día el pago de un renting, que te facilitan la entrada en un piso si está al día el alquiler, etc.

En fin, desde mi punto de vista, **es la revolución contable**. Yo que he tenido que lidiar en el pasado con los libros contables manuales (sin raspaduras…), con la contabilidad por decalco, con máquinas con tarjetas perforadas, con contabilidad con ordenador personal, ...

Lo veo claro, pasaremos de la contabilidad tal cual la conocemos a la contabilidad basada en esta tecnología, que además tiene como valor añadido la trasparencia sobre todas las transacciones que seguro que será muy satisfactoria para la Agencia Tributaria.

4 BIBLIOGRAFÍA

• Martín Fernández; Alonso Rvenga, J.M; Anaya Martín. F; Aneiros Pereira. J; Badenes Pla. N; Matrín Alonso. J; Martín Salcines. F; Rodríguez Márquez. J; Salido Gusi. J

• "*Todo sobre Bitcoin: aspectos económicos, fiscales, contables y administrativos*" (2015). Francis Lefebvre, Madrid.

• Márquez Solís, S. (2015) "*Bitcoin: Guía completa de la moneda del futuro*". Ra-ma, Madrid.

• Juan Carlos Galindo y Basilio Ramírez (2017) "*BIT COIN ¿AMENAZA U OPORTUNIDAD?*"

Apoyo web
Sobre bloques caducados:

• https://www.oroyfinanzas.com/2015/09/que-es-bloque-huerfano-bitcoin-cuando-utiliza/

•http://www.eleconomista.es/empresas-finanzas/noticias/7782103/08/16/Economia-Santander-se-une-a-cinco-entidades-para-promover-el-uso-de-dinero-digital-entre-entidades-financieras.html

•http://www.blogdelaspersonasreales.com/digitalizate/cadena-de-bloques-tecnologia-para-un-mejor-sistema-financiero/

5 VOCABULARIO BÁSICO

Criptomoneda:
También denominadas criptodivisas o monedas virtuales son medios digitales de intercambio.

Criptografía:
La criptografía es la rama de las matemáticas que nos permite crear pruebas matemáticas que proporcionan altos niveles de seguridad. En el caso del Bitcoin, la criptografía se utiliza para hacer imposible que alguien pueda gastar los fondos del monedero de otro usuario o que se pueda corromper la cadena de bloques. También es utilizada para encriptar un monedero, de manera que no se pueda utilizar sin una contraseña.

Bitcoin:
Es una moneda que sirve para intercambiar bienes y servicios. Sin embargo, a diferencia de otras monedas, Bitcoin es una divisa electrónica, un protocolo y un software. La conjunción de estos componentes permite la realización de transacciones casi instantáneas y pagos en todo el mundo con unos niveles altos de eficiencia, seguridad y facilidad de intercambio, así como con unos bajos costos, o incluso nulos, de procesado de dichas transacciones. Se trata de una moneda descentralizada, por lo que nadie la controla.

BTC:
Es la unidad común de la moneda Bitcoin.

Bloque:
Es un registro de la cadena de bloques que contiene confirmaciones de transacciones pendientes. Aproximadamente, cada 10 minutos -en promedio- un nuevo bloque que incluye nuevas transacciones se anexa a la cadena de bloques a través de la minería. En ocasiones puede suceder que un bloque quede caducado o huérfano:

- **Bloque caducado:** se forman habitualmente cuando dos mineros consiguen resolver un bloque con pocos segundos de diferencia. De tal forma que, en ese momento, ambos emiten sus bloques válidos a la red. Ambos mineros están en lo cierto, sus bloques son válidos y, por lo tanto, ambos tienen derecho a recibir la recompensa (coinbase) asociada a su bloque, la cual emiten. Sin embargo, algunos nodos recibirán un bloque antes que el otro, y comenzarán a resolver el siguiente bloque basándose en el hash del que hayan recibido primero. Por otro lado, habrá otros nodos que recibirán el otro bloque primero. Y, por lo tanto, tendrán en cuenta el hash de éste para resolver el siguiente bloque. En ese momento, ambos bloques válidos están en el mismo nivel de la cadena de bloques y crearán lo que se conoce como una bifurcación de la cadena de bloques ocasional o temporal.

Finalmente, un minero produce otro nuevo bloque hijo de uno de los dos bloques competidores que habían sido minados simultáneamente. Y es en ese momento cuando el resto de los nodos descartan el otro bloque, ya que para resolver el siguiente bloque deben elegir la cadena de bloques más extensa, o lo que es lo mismo, con más dificultad. Estos bloques, rechazados en el siguiente nivel de la cadena.

- **Bloque huérfano:** es un bloque que ha sido resuelto correctamente por el minero y es completamente válido, está propagado por la red y está en nodos, pero estos todavía no han sido capaces de asignarle un padre. En esta situación, los nodos van almacenado los bloques a los que no han sido capaces de asignar padre en lo que se denomina como piscina de bloques huérfanos, de esta manera se sigue un registro para llevar control y de donde solo sale el bloque cuando se consigue enlazar con su bloque padre.

Cadena de bloques:
Es un libro de registro de datos: un libro de contabilidad digital de transacciones, acuerdos, contratos… cualquier otra cosa que necesite ser registrada de manera independiente y verificada.

La gran característica de este libro de contabilidad es que no se almacena en un solo sitio, sino que se distribuye a través de varios, cientos o incluso miles de computadoras de todo el mundo, dando acceso a cualquier persona de la red a una versión actualizada.

Los registros generales se amontonan en "bloques" y luego se unen criptográficamente y cronológicamente a una "cadena" que utiliza complejos algoritmos matemáticos. Cada bloque recibe una firma digital única. Una vez actualizado, el libro no se puede alterar ni cambiar, solo se pueden añadir cosas, y se actualiza para todo el mundo en la red al mismo tiempo.

La naturaleza distributiva de la base de datos de la cadena de bloques implica que es más difícil para los hackers atacarla: tendrían que acceder a cada una de las copias de la base de datos simultáneamente para tener éxito. También mantiene los datos seguros y privados porque el resumen criptográfico no puede volver a convertirse en datos originales.

Hashing:
Proceso de encriptación realizado por muchos ordenadores diferentes. Si todas coinciden con la respuesta, cada bloque recibe una firma digital única.

Nodo:
La tecnología en la red Bitcoin está basado en una red distribuida, es decir, que cada computadora conectada a la red contiene la misma información que otra por lo que no responde a un servidor central. Por lo tanto, un nodo es un ordenador que tiene descargado el software Bitcoin QT o Bitcoin Core para participar en la red entre pares (P2P).

Con el fin de validar y transmitir las transacciones, Bitcoin debe transmitir mensajes a través de una red utilizando "nodos".

Mediante el uso de un número de nodos seleccionados al azar, la red puede reducir el problema de doble gasto cuando un usuario intenta pasar el mismo Bitcoin dos veces. Aunque los nodos son iguales, pueden asumir diferentes roles, dependiendo de la funcionalidad que están apoyando. A mayor número de nodos, más segura es la red.

A diferencia de la minería Bitcoin, donde los participantes son recompensados por confirmar transacciones, ejecutar un nodo de Bitcoins no proporciona ninguna recompensa en Bitcoins, el único beneficio para alguien en ejecutar un nodo es para ayudar a proteger la red.

P2P:
Son redes descentralizadas, donde no existe ninguna máquina que actúe como servidor central, no hay ni clientes ni servidores fijos, sino nodos que se comportan como iguales, tanto sirviendo información como consumiéndola con otros nodos de la red. Estos nodos pueden aparecer y desaparecer en cualquier momento, pudiendo conectarse o desconectarse del sistema sin que esto afecte a la red en su conjunto que sigue siendo capaz de funcionar sin ningún problema.

La red Bitcoin implica una red de ordenadores en todo el mundo que constantemente retransmite y transmite nuevas transacciones entre sí. Cada ordenador en esta red es un nodo que tiene descargado la cadena de bloques (Blockchain) completa.

Firma:
Una firma criptográfica es un mecanismo matemático que permite a alguien demostrar su propiedad. En el caso de Bitcoin, un monedero Bitcoin y su clave (s) privada está vinculada por algún tipo de magia matemática. Cuando su programa de Bitcoin firma una transacción con la clave privada correspondiente, toda la red puede ver que la firma coincide con los Bitcoins gastados. Sin embargo, no hay forma de que el mundo descubra la clave privada para robar sus Bitcoins.

Fork:
También conocidos como clones del código fuente original, se basan en la tecnología de Bitcoin para funcionar. Existen en cualquier tipo de desarrollo de software y no son patrimonio exclusivo del proyecto Bitcoin. Los forks suelen dividirse en tres tipos:

1. **Operacionales o Blockchain forks.** – Por la naturaleza descentralizada de Bitcoin, puede ocurrir que los nodos de la red tengan copias desactualizadas de la cadena de bloques y que estas no sean consistentes entre ellas, debido a que los bloques llegan a cada nodo en espacios temporales diferentes, lo que provoca que existan diferentes cadenas de bloques en el tiempo.

2. Accidentales. – Se deben a errores que aparecen en el código a consecuencia de una actualización errónea que los propios desarrolladores cometen. Cuando esto pasa, puede suceder lo siguiente:

- No sucede nada: el error se detecta antes de que ningún nodo se actualice al nuevo software, se corrige y se pone a disposición de todo el mundo la nueva versión.
- Actualizan al nuevo software: entonces habrá nodos en la red Bitcoin funcionando con una versión del cliente y otros con otra versión. La cadena de bloques que los nodos van creando en el proceso de minería, se bifurcará y aparecerán dos nuevas cadenas de bloques diferentes, una perteneciente al código original y otra perteneciente al código con errores.

Esto puede conllevar la pérdida de dinero. Bitcoin solamente tiene una cadena de bloques válida y en el caso de bifurcación hay que elegir cual es la correcta. Los desarrolladores tienen que crear una corrección en el código y esta tiene que distribuirse entre los nodos para que surta efecto; si mientras tanto hay transacciones que acaban en una cadena que luego no será válida, esas monedas podrían perderse.

3. Bifurcaciones duras (hard forks). – Son cambios que se introducen en Bitcoin que presentan incompatibilidades con las versiones de código anteriores y que acaban, invariablemente, con el abandono de la cadena antigua, y la variación a una nueva cadena de bloques, que tiene que ser aceptada por consenso.

Por Basilio Ramírez Pascual

The Matrix Tributario