



# NOTA DE FUTURO 1/2017

30 de enero de 2017

Miguel Ángel Fernández, Fernández, y Selene Pisabarro García\*

## Blockchain: cadena de bloques

### Blockchain:

### *Cadena de bloques*

#### De forma sencilla

*Blockchain* (Cadena de Bloques en español) podría ser definido de manera sencilla como un fichero compartido por miles de ordenadores que imposible de alterar de forma malintencionada. Para falsificar un dato de este sistema sería necesario que en más de la mitad de los usuarios introdujeran esa variación al mismo tiempo, algo prácticamente imposible. En el caso de que los datos sean alterados legítimamente, se sincronizarán de modo automático con todos los ficheros duplicados en los dispositivos en los que se encuentre presente este sistema. En una sola frase: se trata de un registro distribuido que es resistente a la sincronización y sin necesidad de confianza entre los miembros que lo conforman<sup>1</sup>. La ventaja del *blockchain* es que cada usuario está vinculado a una persona real como si fuera una cuenta bancaria, por lo que vincula unívocamente a cada usuario<sup>2</sup>.

Concretamente, el *blockchain* es un nuevo modelo de organizar un negocio que ha evolucionado aunque es necesario gestionar la seguridad, exigiendo menos coste de las auditorías para las empresas a la hora de la ejecución de los contratos.

---

1Bit2me. "¿Qué es la Cadena de Bloques (Blockchain)?". *Bit2me*. S.d. [On line] [Disponible en: <http://blog.bit2me.com/es/que-es-cadena-de-bloques-blockchain/>].

2 Pastor, Javier. "Para qué se está usando blockchain más allá de bitcoin". *Xataka*. S.d. [Disponible en: <http://www.xataka.com/empresas-y-economia/para-que-se-esta-usando-blockchain-mas-alla-de-bitcoin>]

\* Alumnos en prácticas en el Centro de Análisis y Prospectiva de la Guardia Civil (CAP)

Las opiniones contenidas las notas CAP son responsabilidad de sus autores, sin que reflejen necesariamente la opinión del Centro de Análisis y Prospectiva de la Guardia Civil



### A nivel técnico:

El funcionamiento básico del *blockchain* a nivel técnico se basa en el registro de todas las transacciones agrupadas en paquetes que se guardan en bloques que más tarde los “mineros” verificarán. Estos mineros son ordenadores encargados de aportar poder computacional a esta red y de verificar las operaciones que en

ella se realizan. La información será posteriormente integrada en una cadena validada y distribuida por los nodos que conforman el sistema.

Los bloques están integrados por el conjunto de transacciones ya confirmadas, más información adicional que se incluye en esa cadena. Esos bloques forman parte de la cadena, excepto el bloque generatriz que comienza este sistema. Cada bloque está formado por un código alfanumérico que lo enlaza con el anterior, el paquete de transacciones que incluye (identificado con un número determinado por diferentes factores) y otro código alfanumérico que lo enlaza con el siguiente bloque.

Otro concepto clave es el de nodo, un ordenador conectado a la red que utiliza un software que almacena y distribuye una copia actualizada del *blockchain* a tiempo real. Cada vez que uno de estos bloques se completa, se comunica a todos los nodos, que se modifican al mismo tiempo<sup>3</sup>. Cada operación dura un promedio de entre 6 y 11 minutos<sup>4</sup>, lo que puede resultar un poco lento para los usuarios. En el caso de que quieran agilizar el proceso, la transacción será menos segura.

### Sus utilidades:

Este sistema nace como el siguiente paso a la creación del, la moneda más popular en la compra electrónica y la alternativa a la moneda tradicional. En el caso de que se pudiera copiar de la misma manera que se hace con otros archivos, como fotografías o canciones, el sistema se vería completamente desvirtuado. Para ello es necesario la existencia de un libro de contabilidad compartido e infalible: el *blockchain*<sup>5</sup>. A pesar de que el Fondo Monetario Internacional no confiaba en este tipo de cambio y desechaba su utilidad, ahora su directora, Christine Lagarde, cree

---

<sup>3</sup> *Ibid.*

<sup>4</sup> Según la página web Blockchain.info, que ofrece información de los tiempos de espera.

<sup>5</sup> *Ibid.*

que las instituciones financieras deberán adoptar este tipo de tecnologías digitales<sup>6</sup>. Incluso advirtió de que en cinco años estas instituciones deberían estar adaptadas, ya que se trata de herramientas útiles.

Blockchain no solo puede ser un avance determinante para el sector de las finanzas (compra de bonos, acciones o transmisiones de propiedad<sup>7</sup>), sino para las telecomunicaciones o el sector público entre otros. Esto reside en gran parte en su capacidad de probar una identidad, ya que permite comprobar que una persona o empresa es quien dice ser<sup>8</sup>. Otra de sus utilidades sería la posibilidad de elaborar *smart-contracts* o contratos inteligentes entre personas, entidades o máquinas. Sin embargo, es necesario aún que se desarrolle para simplificar el proceso y poder llegar de esta forma a la suscripción de contratos digitales sin la necesidad de la supervisión de un verificador<sup>9</sup>.

Lagarde se muestra expectante ante el grado de confidencialidad que pueda ofrecer el *Blockchain*. Así, afirma que los supervisores se encargarán de revisar los mecanismos debido a que puede ser un riesgo para la legalidad<sup>10</sup>.

### En relación con la seguridad:

Para valorar el verdadero alcance de este nuevo sistema, hay que tener en cuenta que cualquier actividad hecha en internet se basa en la confianza en una autoridad central. Por esta razón, la seguridad en la red es, hoy día, un caos, dado que todos los servicios a los que se confían los datos personales pueden ser manipulados<sup>11</sup>. En cambio, con *Blockchain*, existen menos riesgos una vez que se han validado las acciones mediante un consenso y se han escrito en el controlador. Esto permite que el servicio sea transparente entre los usuarios, así como más rápido y barato. Además, los participantes tienen la posibilidad de cambiar las descripciones de los activos y pueden obtener datos casi a tiempo real, aunque sin conocer la fuente de origen de la información que proviene del

---

6 Reddy, Sudeep. "Interview. Christine Lagarde: 'Automation could open up new jobs'". *The Wall Street Journal*. 3 Octubre 2016. [video on line] [Disponible en: <http://www.wsj.com/video/christine-lagarde-automation-could-open-up-new-jobs/A9EC8DCC-7577-4755-AF63-1EE701413028.html>]

7 Arrieta, E. "Blockchain, la última revolución tecnológica". *Expansión*. 18 Diciembre 2015. [on line] [Disponible en: <http://www.expansion.com/economia-digital/innovacion/2015/12/18/56704eb5e2704e416a8b4684.html>]

8 Tena, María. "Blockchain: las claves para entender, por fin, su importancia. BBVA. 2 Jun. 2016. [On line] [Disponible en: <https://www.bbva.com/es/noticias/ciencia-tecnologia/tecnologia/las-claves-entender-fin-la-importancia-blockchain/>].

9 *Ibid.*

10 Hazzlit, Robert. "Bancos adoptarán criptomonedas en 5 años, dijo la directora del FMI". *Diario Bitcoin.com*. 10 Mayo 2016. [on line] [Disponible en: <http://www.diariobitcoin.com/index.php/2016/10/05/bancos-adoptaran-criptomonedas-en-5-anos-dijo-directora-del-fondo-monetario-internacional/>]

11 *Ibid.*

controlador. Esto permite que los usuarios tengan una mayor confianza respecto a la información que les llega<sup>12</sup>, a pesar de que no significa que la facilidad de las transacciones permita el completo anonimato, ya que salvaguarda los datos para verificar que el dinero procede de una fuente legítima.

### Blanqueo:



Este nuevo sistema puede ayudar a prevenir delitos financieros. Esta capacidad reside en que *blockchain* permite saber de dónde surge el dinero y hacia dónde va. Además de que la moneda con la que se realizan las operaciones, el *bitcoin*, facilita la identificación del usuario por lo que es casi imposible que el crimen organizado intente cometer fuga de capitales en países con muchas restricciones financieras<sup>13</sup>. Incluso la empresa Deloitte afirma que *blockchain* es una manera de identificar intentos de fraude, ya que los datos pueden ser analizados con el objetivo de identificar actividades criminales<sup>14</sup>.

La nueva directiva de pagos europeos, PSD2, impone que todos los pasos de una transacción (proceso técnico, gastos asociados y actores involucrados) deben ir documentados<sup>15</sup>. En este proceso, *blockchain*, es un sistema eficiente para registrar de forma segura los pasos antes mencionados. Los procedimientos de las transacciones quedan registrados, por lo que no deja modificar la información de manera maliciosa y permite que la información sea visible para todos los usuarios pertenecientes a la cadena. Para ello se han establecido una serie de criterios de autenticación a cada inicio de pago. Es en este proceso donde *Blockchain* podría ser de gran utilidad, ya que permite establecer una comprobación eficiente de los datos. Cada vez que se comienza una transacción, el sistema genera información concreta sobre el usuario, y proporciona un *token* de seguridad que podría usarse para firmar digitalmente<sup>16</sup>.

---

12 Brakeville, Sloane y Perepa, Bhargav. "Fundamentos básicos de Blockchain: introducción al negocio". IBM. 4 Noviembre 2016. [on line] [Disponible en: <http://www.ibm.com/developerworks/ssa/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html>]

13 Irene Liñán. "¿Un muro de contención contra el blanqueo?". *Cadena SER*. 23 Mar. 2016. [On line] [Disponible en: [http://cadenaser.com/programa/2016/03/24/hora\\_14\\_fin\\_de\\_semana/1458810903\\_023942.html](http://cadenaser.com/programa/2016/03/24/hora_14_fin_de_semana/1458810903_023942.html)].

14 Prablem Bajpai. "How blockchain can reduce money laundering?". *Nasdaq*. 21 Nov. 2016. [On line] [Disponible en: <http://www.nasdaq.com/article/how-blockchain-can-help-reduce-money-laundering-cm712251>].

15 Atmira. "Blockchain: Tendencias de transformación digital". *Atmira. S.d.* [On line] [Disponible en: <http://www.atmira.com/documents/10180/43613278/BLOCKCHAINBROCHURE.pdf/10a9bdde-e9c6-4461-bdeb-ee523c7edce8>].

16 *Ibid.*

## BIBLIOGRAFÍA

Arrieta, E. "Blockchain, la última revolución tecnológica". *Expansión*. 18 Diciembre 2015. [on line] [Disponible en: <http://www.expansion.com/economia-digital/innovacion/2015/12/18/56704eb5e2704e416a8b4684.html>]

Atmira. "Blockchain: Tendencias de transformación digital". *Atmira. S.d.* [On line] [Disponible en: <http://www.atmira.com/documents/10180/43613278/BLOCKCHAINBROCHURE.pdf/10a9bdde-e9c6-4461-bdeb-ee523c7edce8>].

Bit2me. "¿Qué es la Cadena de Bloques (Blockchain)?". *Bit2me. S.d.* [On line] [Disponible en: <http://blog.bit2me.com/es/que-es-cadena-de-bloques-blockchain/>].

Brakeville, Sloane y Perepa, Bhargav. "Fundamentos básicos de Blockchain: introducción al negocio". *IBM*. 4 Noviembre 2016. [on line] [Disponible en: <http://www.ibm.com/developerworks/ssa/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html>]

Hazzlit, Robert. "Bancos adoptarán criptomonedas en 5 años, dijo la directora del FMI". *Diario Bitcoin.com*. 10 Mayo 2016. [on line] [Disponible en: <http://www.diariobitcoin.com/index.php/2016/10/05/bancos-adoptaran-criptomonedas-en-5-anos-dijo-directora-del-fondo-monetario-internacional/>]

María Tena. "Blockchain: las claves para entender, por fin, su importancia. 2 Jun. 2016. [On line] [Disponible en: <https://www.bbva.com/es/noticias/ciencia-tecnologia/tecnologia/las-claves-entender-fin-la-importancia-blockchain/>].

Pastor, Javier. "Para qué se está usando blockchain más allá de bitcoin". *Xataka. S.d.* [Disponible en: <http://www.xataka.com/empresas-y-economia/para-que-se-esta-usando-blockchain-mas-alla-de-bitcoin>]

Prabem Bajpai. "How blockchain can reduce money laundering?". *Nasdaq*. 21 Nov. 2016. [Online] [Disponible en: <http://www.nasdaq.com/article/how-blockchain-can-help-reduce-money-laundering-cm712251>].

Reddy, Sudeep. "Interview. Christine Lagarde: 'Automation could open up new jobs'". *The Wall Street Journal*. 3 Octubre 2016. [video on line] [Disponible en: <http://www.wsj.com/video/christine-lagarde-automation-could-open-up-new-jobs/A9EC8DCC-7577-4755-AF63-1EE701413028.html>]