¿Qué es el “blockchain” y qué funciones tiene?

3 de mayo de 2019

Autor: Arnie Zareei Bogoya
Miembro del equipo de trabajo del Proyecto Edufinet

Hace tiempo, hablando de inflación con mi sobrino, le pregunté si conocía el país de Zimbawe. Él, dentro de su desconocimiento, desbloqueó su *iPad* y adivinen de dónde sacó su fuente de información. Correcto, de *Wikipedia*.

Cuando era pequeño, recuerdo que ante cualquier duda que tuviese acudía a la enciclopedia, supongamos la Enciclopedia Hispánica, en la que podía encontrar toda la información que necesitase. El funcionamiento era muy sencillo, ya que sólo tenía que buscar la letra por la que comenzaba el concepto en cuestión y ahí encontraría toda la información sobre esa palabra (esos volúmenes eran mi *Wikipedia*).

El sistema descrito es un sistema centralizado, en el que la Enciclopedia Hispánica contrata a un número de contribuidores para crear el contenido y a los comerciales que lo venden, y solo pueden acceder a la información aquellos que tienen la enciclopedia. Con *Wikipedia*, el acceso a la información es descentralizado por lo que cualquiera puede contribuir y puede leer la información, dando como resultado una media de más de 100.000 editores activos. La otra gran diferencia es la velocidad. La próxima vez que vean un evento en directo, por ejemplo, deportivo, hagan la prueba. Así, comprobarán lo rápido que se actualiza la información en la página de *Wikipedia*. *Wikipedia* es, por tanto, una muestra de cómo Internet ha cambiado nuestro mundo y ha descentralizado la información.

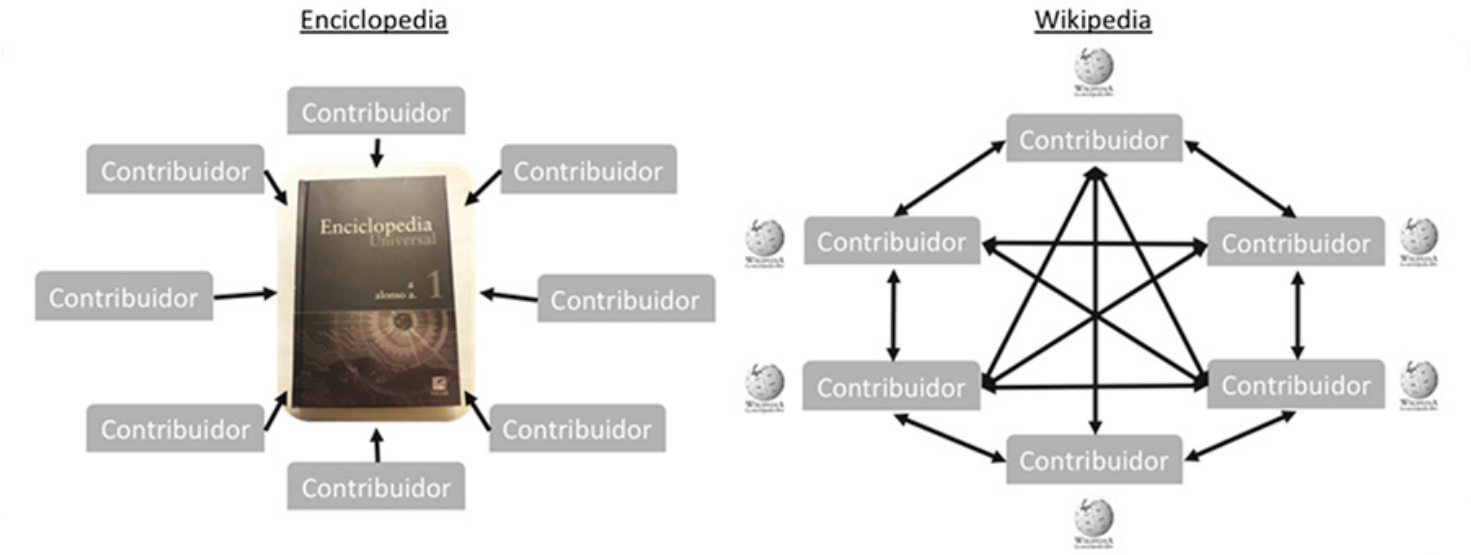

Ilustración 1. Información centralizada e información descentralizada. Fuente: elaboración propia.

En 2007 comenzó la crisis financiera y, como consecuencia, un sector de la población perdió parcialmente la confianza en el sistema financiero, concretamente en los bancos.

En 2009 se lanzó un experimento para ver si se podían establecer sistemas de registro descentralizados, como alternativa a los predominantes, en los que unas autoridades centrales acaparaban su funcionamiento. Una de las manifestaciones de este experimento fue *Bitcoin*.

Para entender cómo funciona *Bitcoin*, tenemos que saber qué es el libro mayor que contabiliza las transacciones. Este libro registra las entradas y las salidas de dinero y se obtiene como resultado el importe en ese libro mayor, que funciona de modo similar a una cuenta bancaria. Un servicio centralizado registra las operaciones, como las de *Verse* o *Paypal*, por ejemplo, y se encarga de verificar las entradas y las salidas de dinero y el saldo a la fecha de consulta. En un sistema descentralizado sucede lo contrario, no hay un sistema central que verifica que la información es correcta, hay miles de ordenadores conectados en el mundo actualizando y verificando la información del libro mayor, y aquí es cuando entra en juego la tecnología del “blockchain” o cadena de bloques.

Fecha	Descripción	Ingreso	Salida	Saldo
01/11/N	Saldo inicial	3.000€		3.000€
30/11/N	Ingreso de Paula	1.000 €		4.000€
01/12/N	Pago a Francisco		500€	3.500€
31/12/N	Ingreso de María	1.500€		5.000€

Tabla 1. Libro Mayor. Fuente: elaboración propia

Cuanta más lotería compre, más probabilidades tendrá de ser el afortunado, y así sucede con la "minería"; mientras más energía utilice y más ordenadores tenga descifrando el código necesario para actualizar el sistema de "blockchain", más posibilidades habrá de ser quien descifre el código y así llevarse la recompensa: alguna unidad de *Bitcoin*. Este código es el que permite añadir el próximo bloque a la cadena y se descifra a través de una fórmula matemática muy complicada; supongamos que el ordenador de Laura lo descifra, entonces ella intentará añadir el bloque a la cadena de bloques. En ese momento, todos los demás ordenadores comprobarán, en primer lugar, que el código de Laura es correcto y, una vez verificado, pasarán a añadir las transacciones. Una vez que los ordenadores lo hayan validado en más de un 50%, el bloque de Laura será correctamente añadido a la cadena de bloques y ella recibirá una recompensa por haber descifrado la fórmula matemática, de esta forma se crean los *Bitcoin*[1]. Esto sucede cada diez minutos, aproximadamente.

Altura	Edad	Transacciones	Minero	Tamaño (Bytes)
570867	4 minutes	2124	Unknown	1.177.345
570866	15 minutes	2412	BTC.com	1.215.870
570865	31 minutes	2201	F2Pool	1.172.917
570864	37 minutes	2541	F2Pool	1.273.338
570863	42 minutes	2844	BitClub Network	1.272.972

Tabla 2. Bloques del sistema blockchain. Fuente: https://www.blockchain.com/es/explorer.

Toda esta información es visible para todo el mundo, y en páginas de Internet como https://www.blockchain.com/es/explorer se pueden observar los bloques que se están creando, así como todas las transacciones que se están añadiendo al libro mayor, miles de ordenadores conectados alrededor del mundo realizando movimientos. Si pulsamos en un bloque podemos ver toda la información relacionada con el mismo: el número de transacciones que aglutina, la edad (representa el tiempo que lleva el bloque en la cadena), el minero (usuario que ha incorporado el bloque), la recompensa recibida por descifrar el bloque, las transacciones incorporadas al libro mayor (acta), etc.

Pensemos en unas elecciones. ¿Cómo sabemos que nuestro voto es válido? Con esta tecnología, desde casa, se podría enviar el voto y si los demás ordenadores conectados no verifican que ese voto es correcto no se incorporaría en el bloque; en cambio, si los ordenadores verifican que ese voto es correcto se añadiría al bloque. "Blockchain" permitiría unas elecciones transparentes en las que todo el mundo puede acceder a la información, preservando el carácter secreto del voto y sin identificar al usuario que envió dicha información, con una autentificación acertada y en tiempo real. Gracias a este sistema se podría saber en el momento de finalización de la jornada quién ganaría las elecciones y no sería necesario gastar grandes cantidades de dinero a la hora de organizarlas.

En el ámbito financiero, una cadena de bloques puede reducir el tiempo de ejecución de las operaciones financieras. Una transferencia internacional puede tardar hasta 4 días laborables en llegar a su destino, pero, en cambio, con un sistema "blockchain" la misma transferencia podría liquidarse en cuestión de minutos, que es el tiempo que transcurre en aceptar la incorporación del bloque a la cadena de bloques. En general, a cualquier producto financiero se le podría aplicar la cadena de bloques, lo que incluso facilitaría la labor de las instituciones que intervienen en el sistema, como, por ejemplo, las cámaras de compensación y liquidación de pagos o de instrumentos financieros.

En abril de 2018, la mayor bolsa de valores de Australia, *Australian Securities Exchange (ASX),* publicó un informe en el que explicaba el reemplazo de su cámara de compensación y liquidación, *the Clearing House Electronic Subregister System (CHESS),* por un sistema basado en el "blockchain". El proceso comenzó en

2015 y estará completamente implementado entre el cuarto trimestre de 2020 y el primer trimestre de 2021.

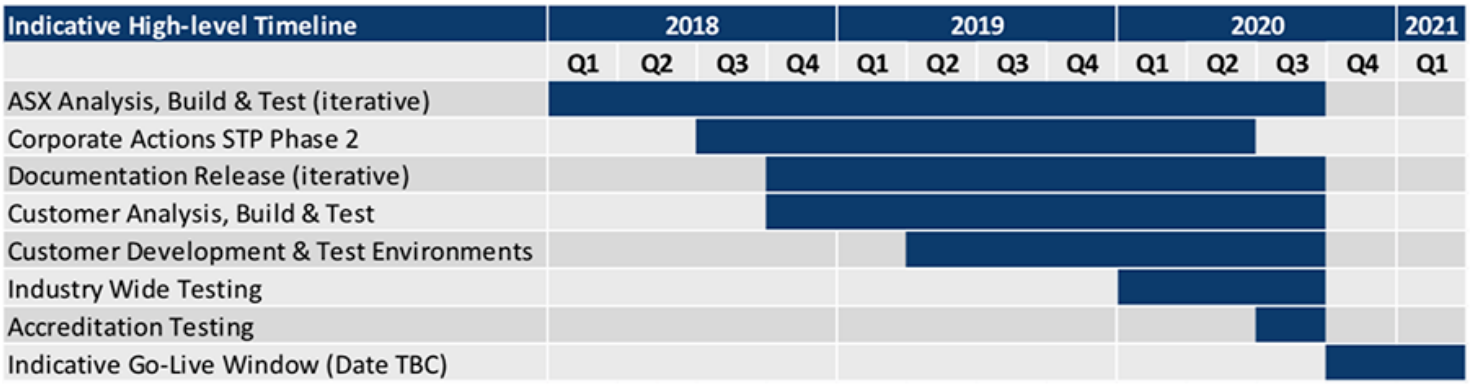

Ilustración 2. Proceso de implementación del sistema «blockchain» en la ASX. Fuente: https://www.asx.com.au/documents/public-consultations/chess-replacement-new-scope-and-implementation-plan.pdf

Pero no todo son ventajas. En noviembre de 2017, por ejemplo, una buena cantidad de unidades de la criptomoneda "Etherum", por valor de varios cientos de millones de dólares, quedó "congelada", no siendo posible su disposición por sus legítimos titulares, debido a un error en la codificación.

En definitiva, aspectos como el riesgo tecnológico o la ciberseguridad, que desarrollaremos en posteriores artículos de este blog, tendrán que ser tomados en consideración por las instituciones financieras, por los reguladores y por los supervisores, para el aprovechamiento de toda la potencialidad de los sistemas descentralizados, en beneficio de las propias instituciones y de sus clientes.

Imagen: Vector de fondo creado por iconicbestiary – www.freepik.es

---

[1] El número de *Bitcoin* es finito hasta la cuantía de 21 millones, por decisión deliberada de su diseñador.