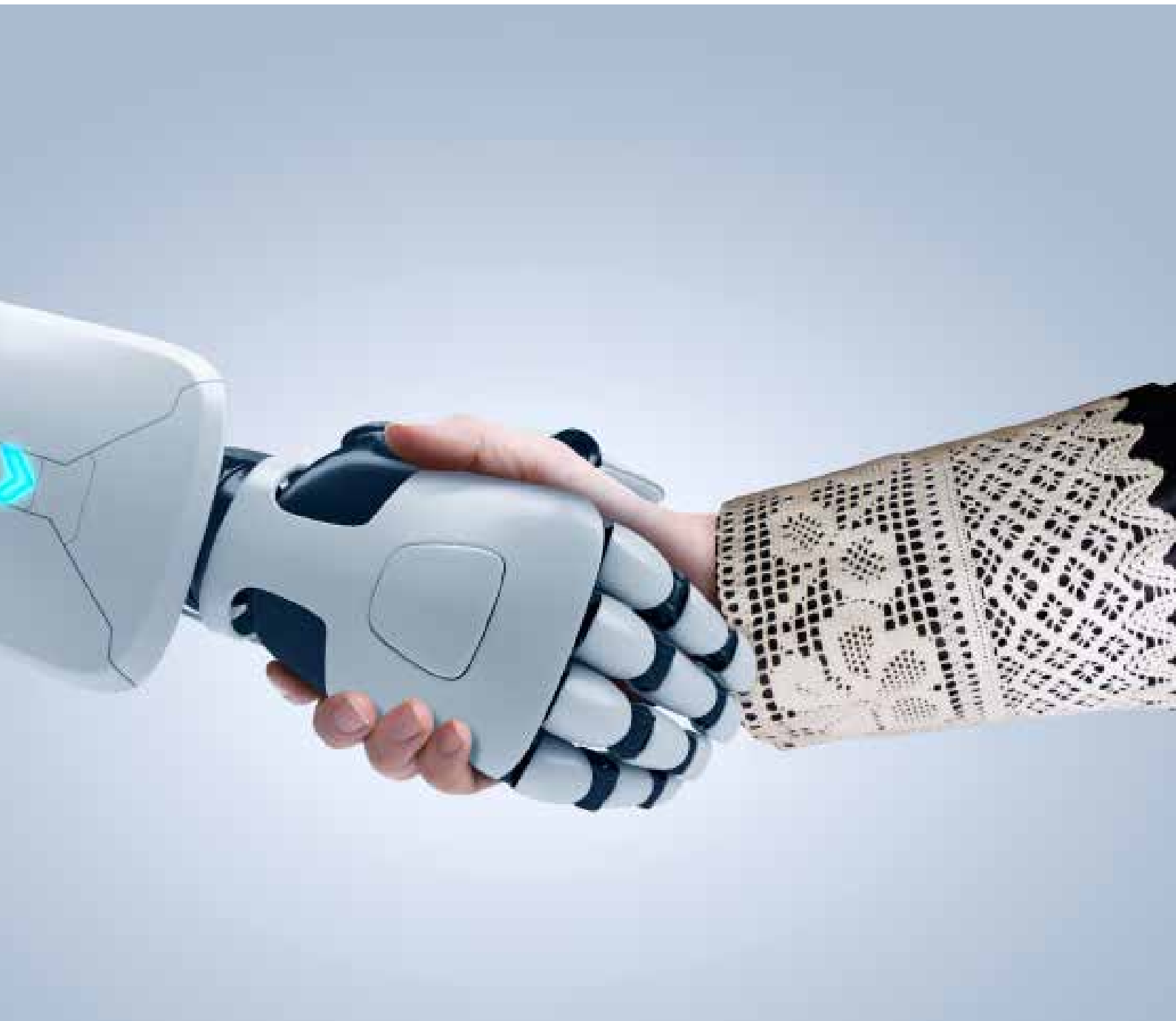
# MÓN JURÍDIC

REVISTA DE L'IL·LUSTRE COL·LEGI DE L'ADVOCACIA DE BARCELONA

**INFORME DE LA JUSTÍCIA 2018**

Núm. 319 · OCTUBRE/NOVEMBRE 2018
WWW.ICAB.CAT



# BLOCKCHAIN: LA TECNOLOGÍA DESCENTRALIZADA QUE POTENCIA LA TRANSPARENCIA

El autor redacta de forma didáctica definiciones de realidades y términos tecnológicos, consiguiendo ponerlas al alcance de profesionales, en este caso de la abogacía, que pueden parecer ajenos a la tecnología.

**Friman Sánchez**
PhD, Doctor en Informática

El estimado lector o lectora se habrá percatado de que Blockchain, Smart Contracts y Digital Ledgers, son términos de gran actualidad. Todos los días podemos encontrar en variados medios de comunicación decenas de artículos y noticias relacionadas con la tecnología de la cadena de bloques, argumentando sobre sus beneficios y su potencial transformador en diferentes sectores como el financiero, la industria, la logística, la salud, los seguros y por supuesto, la administración pública, entre otros muchos sectores.

Estos beneficios están sustentados en el hecho de que la tecnología del blockchain permite desarrollar aplicaciones con la capacidad de asegurar que las transacciones realizadas en un ambiente de negocio en el que interactúan diferentes individuos, organizaciones, empresas o instituciones, se realizan con transparencia y seguridad.

Sin embargo es común encontrarse con la percepción que entender cómo funciona la tecnología del blockchain está fuera del alcance de las personas ajenas al mundo de la tecnología. En este espacio nos proponemos romper con esta idea y asumimos la tarea de describir de la manera más sencilla posible los conceptos básicos que subyacen en la tecnología. En este espacio nos dedicaremos a describir esos conceptos y dejaremos para otra oportunidad, una descripción detallada de las potenciales aplicaciones, los tipos de blockchains existentes, las mejoras tecnológicas que continuamente se proponen por parte de los investigadores y desarrolladores, las implicaciones y retos sociales, económicos, tecnológicos y en muchos casos legales que implica debido al carácter disruptivo de la tecnología.

## ¿QUÉ ES EL BLOCKCHAIN?

Blockchain es descrito con frecuencia como un libro de contabilidad digital en el que cada nueva transacción es anotada al final del libro, por lo tanto es un sistema de almacenamiento de transacciones siempre creciente. La característica fundamental de este libro digital es que asegura que ninguna transacción puede ser alterada o borrada del libro. Las transacciones se anotan en bloques (grupo de transacciones) y cada bloque es "encadenado" al anterior usando un hash criptográfico. Adicionalmente, el blockchain es una estructura de datos descentralizada y distribuida, es decir, que se replica en multitud de ordenadores llamados nodos a través de una red peer-to-peer.

En el caso que estas últimas frases no sean suficientemente claras, los siguientes párrafos explican cada uno de los conceptos mencionados de manera tal que iremos construyendo el conocimiento básico necesario para tener una visión genérica del funcionamiento de la tecnología de la cadena de bloques.

## FUNCIÓN HASH Y HASH CRIPTOGRÁFICO

Una función hash criptográfica es un algoritmo matemático que permite "resumir" una información de entrada de un tamaño cualquiera, en una salida alfanumérica de tamaño fijo llamado hash. Por ejemplo en la figura 1, la información de entrada "Juan da a María 5 euros" es

"resumida" en el hash de 16 caracteres "A1C457D680B-93CE1". Las propiedades de una función hash ideal son diversas, pero solo destacaremos las siguientes:

• Determinismo. Es decir, la misma información de entrada siempre tendrá el mismo hash si se aplica siempre la misma función hash criptográfica. Además, cualquier cambio en la entrada por mínimo que sea, implica la generación de un hash completamente diferente.

• No es factible reconstruir la información de entrada a partir del hash a menos que se prueben todas las entradas posibles, lo cual convierte el proceso en un problema de complejidad intratable.

• No es factible encontrar dos informaciones de entrada con el mismo valor de hash. Esta propiedad permite interpretar el hash como una especie de huella digital de la información.

• La generación de un hash a partir de los datos de entrada implica un coste computacional muy bajo.

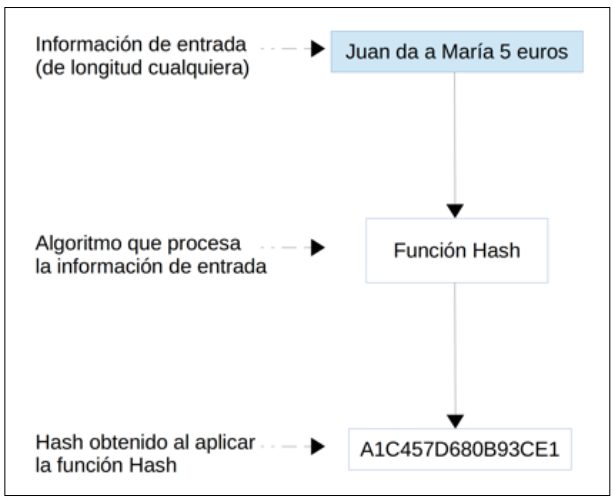



Figura 1: Función Hash criptográfica y Hash

## Los conceptos de bloque y nonce

Con el concepto de hash en nuestro bolsillo, pasamos a describir el concepto de bloque. Un bloque es una agrupación de transacciones. La función hash criptográfica puede aplicarse sobre todo un bloque para obtener un único hash de ese bloque. Recordemos que el tamaño de la información de entrada no implica un cambio en el tamaño del hash calculado. La figura 2 representa un ejemplo de bloque cuyo hash es "37401AF63D801A0E".

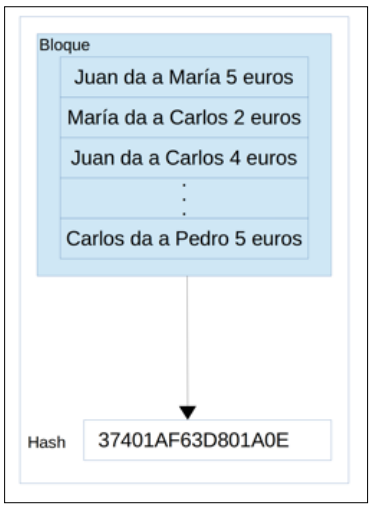



Figura 2: Un bloque y su respectivo hash

Ahora imagine que no estamos interesados en hashes de cualquier tipo, si no en aquellos que tengan una característica particular, por ejemplo deseamos hashes que siempre empiecen por los caracteres 0000. Para lograr este objetivo concatenamos al bloque un número que nos da la posibilidad de generar hashes diferentes cada vez que variamos dicho número. Este número se llama nonce. La figura 3 muestra diferentes hashes obtenidos al utilizar diferentes nonces para un mismo bloque. El procedimiento consiste en ensayar diferentes nonces hasta obtener el hash con la característica deseada (ej: 4 ceros al principio).

## Minado de bloques

Encontrar el hash con la característica deseada es un proceso lento de ensayo y error. No existe ninguna fórmula matemática que permita predecir cuál es el nonce que conduce al hash con dicha característica. Debido a la cantidad de veces que debe ensayarse el procedimiento, este resulta computacionalmente costoso. Por ello a este proceso se le conoce con el nombre de minado de bloques. El único objetivo de generar un hash con la característica descrita es hacer que el proceso sea difícil de reproducir por el tiempo y computación requeridos.

Una vez se logra el objetivo de obtener un hash con la característica deseada, la generación de hashes para dicho bloque se detiene y nos quedamos con ese último. En el ejemplo de la figura 3, se ha logrado obtener el hash "0000801ADCA7E12F" cuando se utilizó el nonce 36574, es decir, después de probar esa cantidad de nonces diferentes. Un bloque cuyo hash posee la característica buscada se denomina bloque firmado.

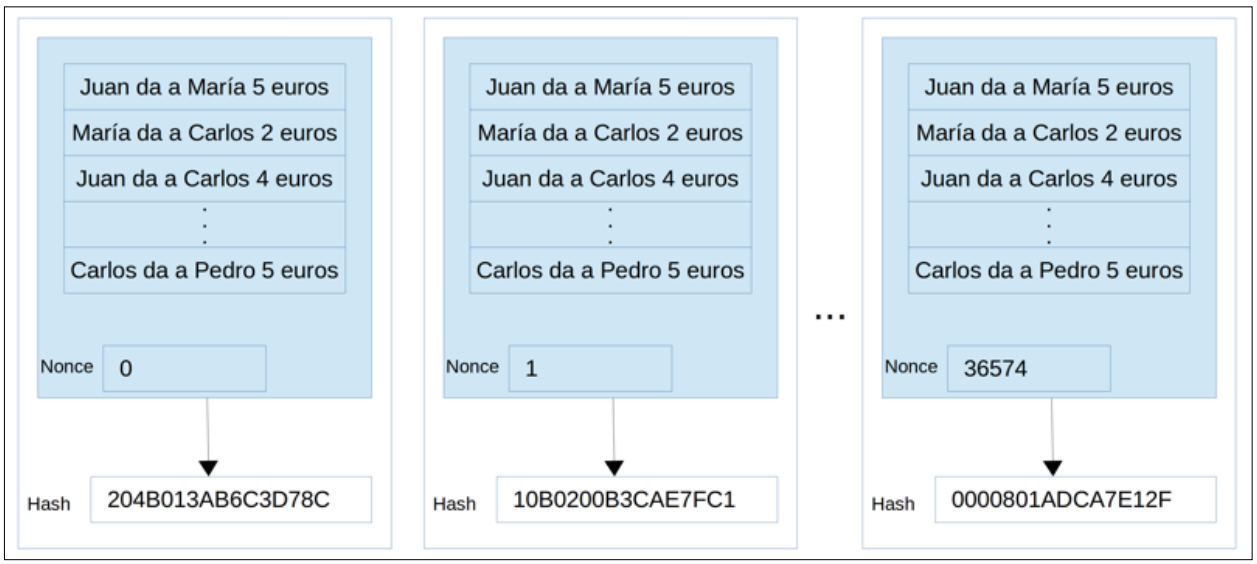



Figure 3: Un bloque con diferentes nonces y por tanto diferentes hashes. El bloque de la derecha contiene la característica deseada de 4 ceros al principio y se obtiene al probar el nonce 36574

## Encadenamiento de bloques

Una vez discutidos los conceptos anteriores, ya estamos en condiciones de avanzar un paso más para entender en qué consiste la cadena de bloques. Imagine que existen muchas transacciones agrupadas en varios bloques que enumeramos consecutivamente como bloques 0, 1, 2, 3, etc. El encadenamiento de los bloques se logra incluyendo el hash del bloque anterior en el bloque siguiente y a partir de ahí se computa el hash correspondiente de dicho bloque, tal y como muestra la figura 4 para una cadena de 4 bloques.

Puede verse que los bloques contienen transacciones diferentes generadas secuencialmente a lo largo del tiempo. Para el bloque 0, al ser el inicial, podemos asumir que el hash previo está compuesto solamente de ceros, a partir de este, se encuentra el nonce que nos permite obtener el hash 0 adecuado. Para el bloque 1, se incluyen las transacciones de este nuevo bloque junto con el hash 0, y se calcula el hash 1 de este bloque. Este procedimiento de encadenamiento se realiza para cada bloque de transacciones que va llegando a la cadena.

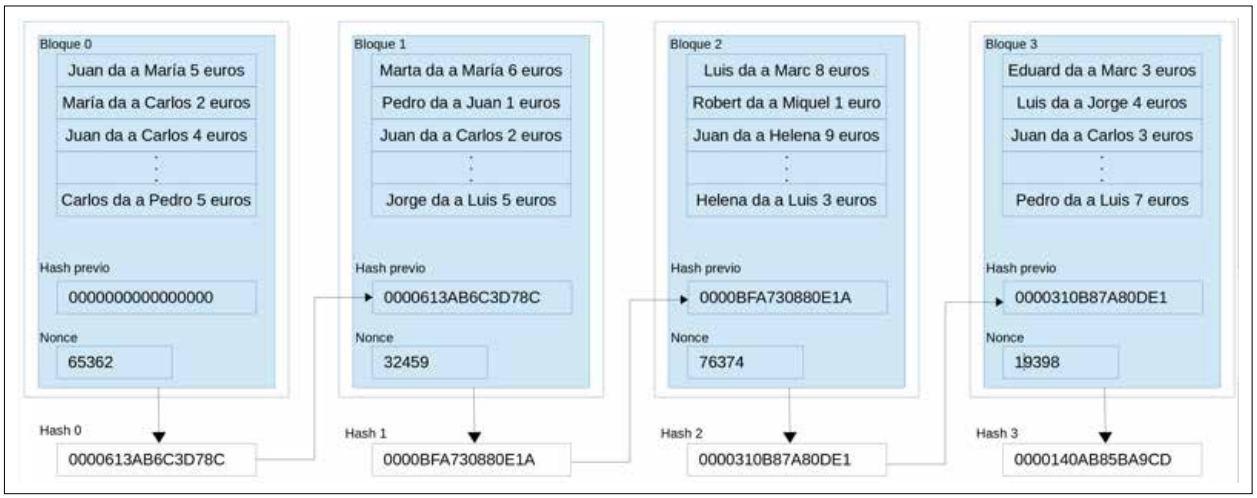



Figura 4: Encadenamiento de bloques a través de los hash calculados para cada bloque.

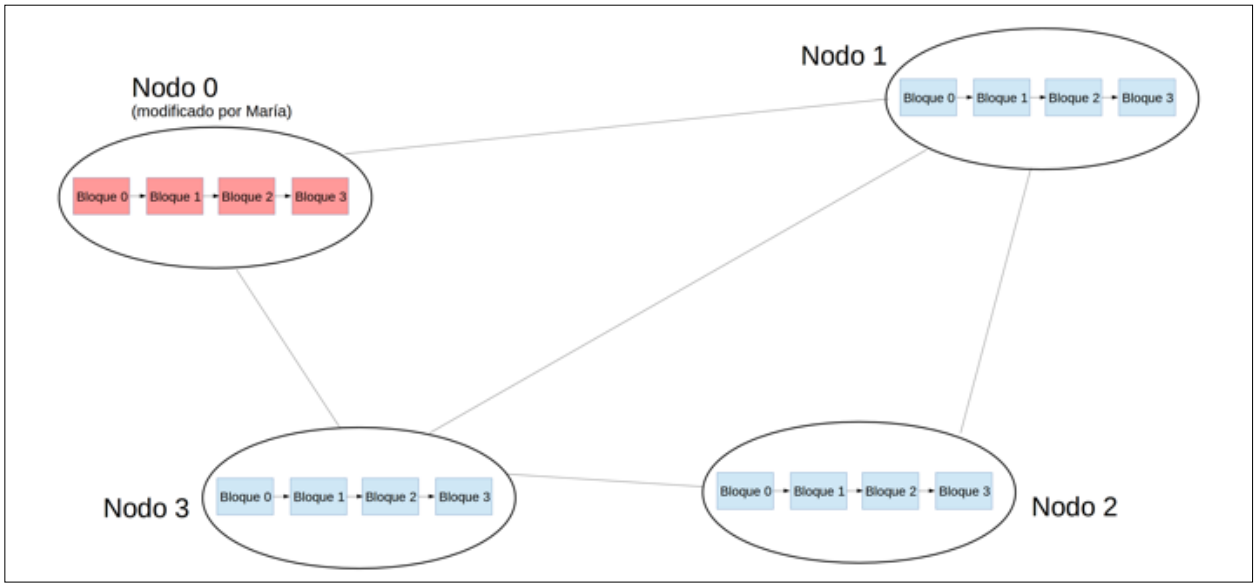



Figura 5: Blockchain distribuido a lo largo de diferentes nodos. Si María ha logrado modificar su propia copia del blockchain es fácil para el resto de la red detectar que dicho nodo no es coherente con el resto.

Una ventaja que debe resaltarse en este punto es que resulta fácil asegurar que los hashes se corresponden con la información del bloque. Recuerde, es difícil generar los hashes con la característica deseada pero una vez generados es muy sencillo verificar que dicho hash ha sido obtenido a partir del bloque al que dice pertenecer. Esto implica que si por alguna razón se intenta realizar un cambio en cualquier bloque, sería fácil detectarlo porque al verificar el hash, se llegaría a la conclusión de que no hay correspondencia. Y dada la concatenación entre bloques, a partir de ese cambio ningún bloque sería coherente con su hash.

## CADENA DE BLOQUES DISTRIBUIDA

Si usted ha llegado hasta aquí, ya ha logrado adquirir los conceptos básicos relevantes para entender el funcionamiento del blockchain. Ahora vamos a discutir la importancia de que el blockchain sea un sistema descentralizado y distribuido. Recuerde que una estructura de datos descentralizada y distribuida significa que está replicada en multitud de ordenadores o nodos a través de una red peer-to-peer.

Imagine que María estuviese interesada en manipular la transacción en favor de Carlos que se almacena en su nombre en el bloque 0 ("María da a Carlos 2 euros"). Supongamos que ella tiene la suficiente capacidad computacional para reescribir la historia desde el bloque 0 hasta el bloque actual en la copia del blockchain que tiene en su ordenador o nodo. Esto implica que debería volver a calcular cada hash de cada bloque para obtener nuevos hashes que cumplan la característica deseada, de tal manera que produciría una nueva versión del blockchain que difiere de la original.

Sin embargo, debido a que el sistema es distribuido, existen muchos nodos que almacenan una copia igual del blockchain, tal y como lo muestra la figura 5. María tendría una copia modificada de los datos, pero el resto de nodos continúa almacenando la versión original y que por lo tanto, contiene la historia real de las transacciones ocurridas. Sería extremadamente complejo para María modificar todas las copias de todos los nodos y mantener la coherencia de la información en toda la red. Se añade a esto el hecho de que constantemente la red está agregando nuevos bloques utilizando un protocolo de consenso definido para ello (que no explicamos en este momento), con lo cual la complejidad en la tarea subversiva de María crece permanentemente.

## EL BLOCKCHAIN ES INCORRUPTIBLE Y TRANSPARENTE

La imposibilidad práctica de alteración o borrado de información en el blockchain que hemos descrito en los párrafos anteriores es una garantía de integridad de la información y transparencia otorgada por la tecnología y que permite a los participantes de la red tener plena confianza en la información que se almacena. Además, dado el carácter descentralizado de la red, se facilita la colaboración o intercambio entre los participantes sin la necesidad de la existencia de una autoridad central o intermediario que de confianza entre las partes.