



**EDUARDO MORA GONZÁLEZ**

## Contenido

1.	INTRODUCCIÓN .....	3
2.	EVOLUCIÓN .....	3
2.1.	INICIOS.....	4
2.1.1.	EL SELLADO DE TIEMPO.....	4
2.2.	PRUEBA DE TRABAJO REUTILIZABLE .....	5
2.2.1.	HASHCASH .....	5
2.3.	INICIO DEL BITCOIN .....	6
2.4.	ETHEREUM .....	7
3.	ELEMENTOS DEL BLOCKCHAIN.....	7
4.	CLASES DE BLOCKCHAIN.....	8
5.	APLICACIONES .....	9
5.1.	CRIPTO-MONEDAS .....	9
5.2.	SISTEMA DE DISTRIBUCIÓN DE FIRMWARE .....	10
5.3.	SEGURIDAD EN BIG DATA MEDIANTE BLOCKCHAIN .....	11
6.	CONCLUSIÓN .....	12
	REFERENCIAS.....	13

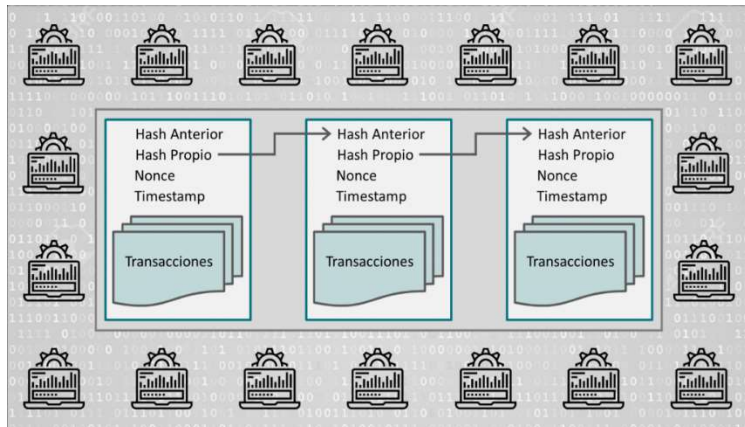
## 1. INTRODUCCIÓN

Blockchain que en español significa, literalmente, cadena de bloques. Es un sistema con el cual se pueden hacer transacciones seguras entre personas en todo el mundo sin necesidad de intermediarios [1].

Su funcionamiento puede resultar complejo de entender si profundizamos en los detalles internos de su implementación, pero la idea básica es sencilla de seguir. En cada bloque se almacena:

- Una cantidad de registros o transacciones válidas,
- Información referente a ese bloque,
- Su vinculación con el bloque anterior y el bloque siguiente a través del hash de cada bloque —un código único que sería como la huella digital del bloque.

Por lo tanto, cada bloque tiene un lugar específico e inamovible dentro de la cadena, ya que cada bloque contiene información del hash del bloque anterior. La cadena completa se guarda en cada nodo de la red que conforma la blockchain, por lo que se almacena una copia exacta de la cadena en todos los participantes de la red.



A medida que se crean nuevos registros, estos son primeramente verificados y validados por los nodos de la red y luego añadidos a un nuevo bloque que se enlaza a la cadena [2].

## 2. EVOLUCIÓN

En este punto se va a hablar sobre la evolución del Blockchain a lo largo del tiempo.

## 2.1. INICIOS

La idea detrás de la tecnología blockchain se describió en 1991, cuando los científicos de investigación *Stuart Haber* y *W. Scott Stornetta* introdujeron una solución computacionalmente práctica para los documentos digitales con sello de tiempo para que no pudieran ser modificados o manipulados.

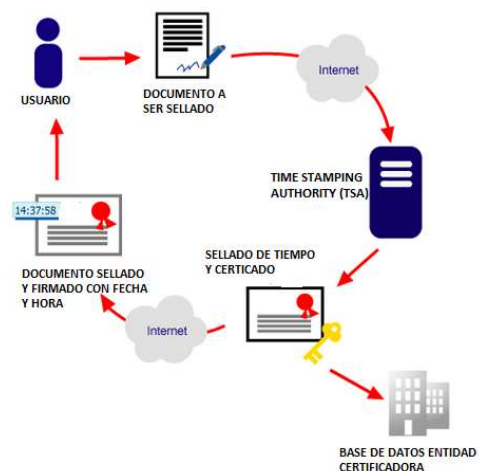
El sistema usó una cadena de bloques con seguridad criptográfica para almacenar los documentos con sello de tiempo y en 1992 se incorporaron al diseño los árboles Merkle, lo que lo hizo más eficiente al permitir que varios documentos se reunieran en un solo bloque. Sin embargo, esta tecnología no se utilizó y la patente caducó en 2004, cuatro años antes del inicio de Bitcoin [3].

### 2.1.1. EL SELLADO DE TIEMPO

Un sellado de tiempo [4] es un mecanismo que permite probar la integridad de una serie de datos. Es decir, permite demostrar que esos datos han existido en un momento determinado, y que no han sido alterados desde entonces.

La integridad es precisamente uno de los requisitos que permiten que un proceso de firma sea seguro y tenga plenas garantías legales para todas las partes.

Las autoridades de sellado de tiempo utilizan una tecnología llamada infraestructura de clave pública o PKI, que permite ejecutar varios tipos de operaciones criptográficas, como por ejemplo el cifrado y descifrado de comunicaciones.



En el caso de aplicar un sello de tiempo a una firma electrónica, el funcionamiento es el siguiente:

1. Cuando se firma un documento, se envía a la Autoridad de Sellado de Tiempo un valor hash que representa los datos del documento firmado, incluidos los datos de la firma (firma encriptada).
2. La Autoridad de Sellado de Tiempo devuelve un hash distinto, que es el sellado de tiempo (que no deja de ser un certificado de tiempo).

3. Con este sello de tiempo se garantiza la integridad de todos los datos que forman parte del documento. Si se modificasen estos datos en algún momento posterior al sellado, éste se rompería.

Todo este proceso hace que se cree un documento probatorio que tenga la siguiente información:

- Los correos electrónicos de solicitante y firmante.
- El nombre de archivo del documento a firmar.
- El lugar y momento exacto en que se ha llevado a cabo la firma, capturado mediante geolocalización.
- Los eventos registrados (envío, apertura, firma, etc.)

## 2.2. PRUEBA DE TRABAJO REUTILIZABLE

En 2004, el informático y activista criptográfico *Harold Thomas Finney* introdujo un sistema llamado *Reusable Proof Of Work* (Prueba de Trabajo reutilizable).

El sistema funcionó al recibir un token de prueba de trabajo no intercambiable o no fungible basado en *Hashcash* y, a cambio, creó un token firmado por RSA que luego podría transferirse de una persona a otra.

Esto resolvió el problema del doble gasto manteniendo la propiedad de los tokens registrados en un servidor confiable que fue diseñado para permitir a los usuarios de todo el mundo verificar su exactitud e integridad en tiempo real [3].

### 2.2.1. HASHCASH

HashCash fue una solución diseñada para combatir el spam generando una prueba de trabajo que permitía verificar que un determinado correo electrónico no era correo basura.

El nombre de HashCash hace mención a una tecnología de Prueba de Trabajo (PoW) que se usó para minimizar el correo no deseado (spam) y los ataques de denegación de servicio (conocidos como DoS o DDoS).

Esta tecnología ganó amplia popularidad gracias a su implementación en el Bitcoin y muchas otras criptomonedas. Su función en las mismas era formar parte del algoritmo de validación de los bloques.

El objetivo de HashCash, es requerir un trabajo de computación para que este sea verificado. Una vez verificado dicho trabajo, se le permite al usuario hacer uso del recurso. El uso en el correo electrónico se basa en añadir un encabezado codificado al correo. Dicho encabezado tiene la información generada por el usuario utilizando el sistema HashCash. Esto es una especie de sello que asegura que el correo ha pasado por la prueba de trabajo. Dicho sello, es un identificador que demuestra que el remitente ha utilizado el procesador durante una pequeña cantidad de tiempo. Pues es la única manera de generar un sello genuino para cada correo electrónico que se desee enviar [5].

### 2.3. INICIO DEL BITCOIN

A finales de 2008, una persona o un grupo con el seudónimo *Satoshi Nakamoto* publicó en una lista de correo de criptografía un libro blanco que introdujo un sistema de efectivo electrónico descentralizado entre pares (llamado Bitcoin).

Basado en el algoritmo de Prueba de Trabajo de *Hashcash*, pero en lugar de utilizar una función de computación confiable de hardware como el RPoW, la doble protección contra gastos en Bitcoin fue proporcionada por un protocolo descentralizado de igual a igual para el seguimiento y la verificación de las transacciones.

El 3 de enero de 2009, Bitcoin nació cuando el primer bloque de bitcoin fue minado por Satoshi Nakamoto, que tuvo una recompensa de 50 bitcoins. El primer receptor de Bitcoin fue *Hal Finney*, recibió varios bitcoins de Satoshi Nakamoto en la primera transacción de bitcoin del mundo el 12 de enero de 2009 [3] (en la foto de abajo se puede ver el detalle de esa transacción).

**TRANSACCIÓN BITCOIN** 50,00 BTC  
f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

Valor de transacción	50,00 BTC	Entradas totales	50,00 BTC
Confirmaciones	623555	Salidas totales	50,00 BTC
Altura	170	Fecha de confirmación	1/11/09, 11:00 PM
Tiempo de recepción	1/11/09, 11:00 PM	Tamaño	275 bytes
Tiempo de bloqueo	0		

**Detalles**

Sin entradas (Monedas recién generadas) ( 50,00 BTC )

→ 1Q2TWHE3GmdB6B2KafqwxXtWAWgFt5jvm3 (10,00 BTC)  
12cbQLTFMXRnSztFkuoG3eHoMeFtpTu3S (40,00 BTC)

## 2.4. ETHEREUM

En 2013, *Vitalik Buterin*, programador y cofundador de la revista Bitcoin, declaró que Bitcoin necesitaba un lenguaje de scripting para crear aplicaciones descentralizadas. Al no lograr un acuerdo en la comunidad, *Vitalik* comenzó el desarrollo de una nueva plataforma de computación distribuida basada en blockchain, Ethereum, que presentaba una funcionalidad de scripting, llamada contratos inteligentes.

Los contratos inteligentes son programas o scripts que se implementan y ejecutan en la cadena de bloques Ethereum; se pueden usar, por ejemplo, para realizar una transacción si se cumplen ciertas condiciones. Los contratos inteligentes se escriben en lenguajes de programación específicos y se compilan en un código de bytes, que una máquina virtual completa de Turing descentralizada, llamada la máquina virtual Ethereum (EVM) puede leer y ejecutar.

Los desarrolladores también pueden crear y publicar aplicaciones que se ejecutan dentro de la cadena de bloques Ethereum. Estas aplicaciones generalmente se denominan DApps (aplicaciones descentralizadas) y ya existen cientos de DApps que se ejecutan en la cadena de bloques Ethereum, incluidas las plataformas de redes sociales, aplicaciones de juegos de azar e intercambios financieros.

La criptomoneda de Ethereum se llama Ether, se puede transferir entre cuentas y se usa para pagar las comisiones de la potencia de cálculo utilizada al ejecutar contratos inteligentes [3].

## 3. ELEMENTOS DEL BLOCKCHAIN

Para conocer hasta qué punto puede llegar la tecnología Blockchain, se requiere conocer los componentes básicos de este. Para una mejor comprensión de sus elementos, nos basaremos en el estudio realizado por *Preukschat* (2017), que destaca principalmente cuatro [6]:


- **Un nodo:** puede ser desde un ordenador personal hasta una mega computadora y aunque no es tan importante la capacidad que debe tener un nodo, lo que sí es fundamental y necesario para su correcto funcionamiento es que todos los nodos deben de tener el mismo software o protocolos para poder comunicarse entre todos los nodos. Sin ello no

podrían conectarse a la red de una Blockchain. Además, puede tener la característica de ser pública, privada o híbrida.

- **Un protocolo estándar:** Un software informático para todo el conjunto de ordenadores puedan comunicarse entre sí a través de la difusión de un estándar común para establecer la comunicación entre los participantes de la red. Uno de los protocolos más conocidos son el SMTP que es el que se utiliza para la recepción y envío de correos electrónicos.
- **Una red entre pares:** También conocido como P2P, una red de nodos (ordenadores) conectados directamente en una misma red. Uno de los más reconocidos sería *UTorrent*.
- **Un sistema descentralizado:** La tecnología Blockchain es un sistema descentralizado y este sistema desarrollado tiene muchas implicaciones para las personas, que, a diferencia de sistemas centralizados, donde toda la información esta manejada y controlada por solo una entidad u organismo, en este nuevo sistema son todos los componentes conectados que lo forman los que controlan este sistema, teniendo todos el mismo rango o jerarquía.

#### 4. CLASES DE BLOCKCHAIN

Existen 4 clases distintas de Blockchain, en la siguiente imagen se ilustra de manera esquemática las características de cada una de estas clases [7]:



	Públicos Bitcoin, Ethereum, Litecoin	Privados Hyperledger, Corda, Quorum	Federados Hyperledger, Corda, Quorum	Blockchain as a Service IBM, Microsoft, Amazon
Cualquiera puede participar	✓	✗	✗	NA
Los participantes actúan, en general, como nodos	✓	✗	✗	NA
Transparencia	✓	≈	≈	NA
Hay un único administrador	✗	✓	✗	NA
Hay más de un administrador	✗	✗	✓	NA



No hay administradores	✓	✗	✗	NA
Ningún participante tiene más derechos que los demás	✓	✗	✗	NA
Se pueden implementar Smart Contracts	✓	✓	✓	NA
Existe recompensa por minado de bloques	≈	✗	✗	NA
Soluciona problema de falta de confianza	✓	✗	≈	NA
Seguridad basada en protocolos de consenso	✓	✗	≈	NA
Seguridad basada en funciones <i>hash</i>	✓	≈	≈	NA
Provee servicios en la nube	NA	NA	NA	✓

✓ Si    ✗ No    ≈ A veces    NA No Aplica

## 5. APLICACIONES

Actualmente el bitcoin es, sin duda alguna, la realización más conocida de la tecnología blockchain. Sin embargo, existe una lista de posibles casos de uso mucho más larga y potencialmente más revolucionaria que el bitcoin. Algunos de estos casos son:

### 5.1. CRIPTO-MONEDAS

Sin una autorización central, blockchain puede diseñarse como una base de datos verdaderamente descentralizada. Por lo tanto, puede actuar como un centro de intercambio confiable entre múltiples entidades, sin requerir que una entidad confíe en otra entidad, o incluso sin un intermediario.

Esto representa una verdadera revolución: en los sistemas de intercambio siempre se ha requerido un intermediario de confianza de todas las partes. Por ejemplo, cuando alguien compra un artículo de segunda mano en una plataforma online, es el responsable de verificar si la transacción se ha realizado con éxito a cambio de un determinado porcentaje y compensar a las partes en caso de fraude.

Para las monedas clásicas, también existe una agencia de gestión de divisas: el Banco Central. Este es el único con el poder suficiente para emitir más unidades monetarias. Estas decisiones generalmente se toman con base en criterios de política

macroeconómica, tales como: estabilidad a largo plazo, metas de inflación, ratios de importación y exportación, etc.

La criptomoneda basada en blockchain también elimina la necesidad de una autoridad central. Los criterios para emitir nuevas unidades monetarias están predeterminados. Por ejemplo, en el caso de Bitcoin, se emite una nueva moneda cada vez que se extrae un bloque (aproximadamente cada 10 minutos) y se devuelve al nodo que extrajo la moneda. Por tanto, la incertidumbre asociada a esta decisión política desaparece. Además, se elimina la posibilidad de que el Estado utilice al banco central para beneficiar a determinados sectores o perjudicar a otros sectores [8].

## 5.2. SISTEMA DE DISTRIBUCIÓN DE FIRMWARE

A medida que Internet de las cosas (IoT) se convierta en una realidad, la cantidad de dispositivos conectados a la red aumentará exponencialmente. Ahora, además de ordenadores y equipos de red, se han conectado a Internet electrodomésticos, equipos de vigilancia y seguridad, diversos sensores, etc. Este nuevo ecosistema, sin duda, proporciona una flexibilidad sin precedentes. Sin embargo, este paradigma también tiene algunos desafíos por resolver. Entre ellos, destaca el campo de la seguridad.

El primer problema de seguridad que aparece en el entorno de IoT es el nivel de supervisión de los equipos. En este sentido, en el entorno IoT, muchos dispositivos no están sujetos al nivel de supervisión que se utiliza en el mundo informático (ordenadores personales o smartphones). Además, debido al bajo costo, muchos de estos equipos no siempre reciben actualizaciones del fabricante con mucha frecuencia (o incluso a veces no están disponibles). Los fabricantes tienen que enviar actualizaciones directamente a millones de dispositivos, y lo hacen incluso después de dejar de fabricar dichos dispositivos durante muchos años, lo que resulta muy caro.

Es probable que esta situación se resuelva mediante blockchain. En este caso, se utilizarán al mismo tiempo sus características de sistema distribuido y transparencia, así como su robustez y fiabilidad. El dispositivo consultará la cadena de bloques para ver si su firmware está actualizado. De lo contrario, pedirán a otros nodos que les envíen una nueva versión.

Una vez recibido, pueden usar el código blockchain para verificar que el firmware no haya sido manipulado, evitando así la intrusión. Una vez implementado, este método será mucho más económico para los fabricantes, y los fabricantes solo necesitan enviar actualizaciones a unos pocos nodos [9].

### 5.3. SEGURIDAD EN BIG DATA MEDIANTE BLOCKCHAIN

Actualmente se utilizan varias tecnologías de big data para analizar blockchain y mejorar su nivel de seguridad. Estas tecnologías pueden deducir la identidad de nodos en criptomonedas, detectar fraudes y mapear flujos de capital reales. Sin embargo, esta relación inversa es aún más prometedora: utilizar la tecnología blockchain para proporcionar seguridad y verificabilidad para el entorno empresarial de big data.

Con el crecimiento explosivo del big data, casi todas las empresas con la menor cantidad de clientes están interesadas en aprovechar al máximo los datos para seguir siendo competitivas. Estos datos generalmente provienen de una variedad de fuentes, tienen diferentes formatos y son utilizados por diferentes departamentos de la empresa en varios procesos. Los peligros de estos sistemas son obvios: el personal interno manipula datos, proveedores malintencionados, corrupción de datos, fallas de almacenamiento y funcionamiento a largo plazo...

En este caso, blockchain puede hacer muchas contribuciones: transparencia, verificabilidad, portabilidad y escalabilidad. A través de blockchain, se puede utilizar un registro transparente y seguro para completar cada adición de datos, cada cambio, cada extracción de uso o cada visualización. Además, los datos pueden ir acompañados de una prueba de integridad de bajo nivel, e incluso en el caso de extracción, tiene una firma específica que permite su trazabilidad.

Estos entornos permiten un cierto grado de seguridad y verificabilidad, suficiente para ser distribuidos en la naturaleza, escalables e interoperables cumpliendo estrictas normativas. Los requisitos legales para la retención de datos ya no son un problema, porque poder inferir el estado de la base de datos en cualquier momento es la esencia del blockchain [10].

## 6. CONCLUSIÓN

Como podemos ver, las posibilidades de blockchain son prácticamente infinitas y afectan a todos los ámbitos de negocio en los que podemos pensar, y algunos nuevos que están por aparecer. Por eso me gustaría acabar este trabajo con la siguiente frase que define todo el proceso de evolución de la tecnología:

***“La tecnología del futuro ya la conocemos, es lo que hoy llamamos ciencia ficción”.***

## REFERENCIAS

1. <https://economytic.com/blockchain/>
2. <https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/>
3. <https://academy.binance.com/es/articles/history-of-blockchain>
4. <https://blog.signaturit.com/es/la-autoridad-de-sellado-de-tiempo-un-cierre-hermetico-para-brindar-mayor-seguridad-a-la-firma-electronica>
5. <https://academy.bit2me.com/que-es-hashcash/>
6. [http://repositorio.ual.es/bitstream/handle/10835/6599/16654\\_TFG%20Blockchain%20Tony.pdf?sequence=1&isAllowed=y](http://repositorio.ual.es/bitstream/handle/10835/6599/16654_TFG%20Blockchain%20Tony.pdf?sequence=1&isAllowed=y)
7. <https://blogs.iadb.org/conocimiento-abierto/es/tipos-de-blockchain/>
8. <https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf>
9. CHRISTIDIS, K. &. (2016). «Blockchains and Smart Contracts for the Internet of Things». IEEE Access, 4, 2292-2303. EtherAPIs: Decentralized, anonymous, trustless APIs. (2017). Obtenido de EtherAPIs: etherapis.io.
10. FARELL, R. (2015). «An analysis of the cryptocurrency industry.» FILECOIN: A Cryptocurrency Operated File Storage Network. (2017). Obtenido de FileCoin: filecoin.io