# BLOCKCHAIN

José Pablo Colindres Orellana

Usac – Facultad de Ingeniería – Escuela de Ciencias y Sistemas

Nota del autor

Blockchain es una tendencia tecnológica en la construcción de sistemas y servicios.

Resumen

En la actualidad, la necesidad y la preocupación de mantener tus archivos e información, ya sea personal, bancaria, etc., de manera segura es mayor. La desconfianza que generan grandes empresas en las que uno debe confiar toda su información (por miedo a que alguien pueda acceder a ella) puede acabarse, eso sí, es una meta de largo plazo. El uso de blockchain ha ido aumentado y revolucionando lo que son las operaciones en línea, asegurando la seguridad y privacidad de información. Esto es posible gracias a la encriptación de los datos y siendo accesible únicamente por el propietario.

*Palabras clave*: Blockchain.

# ¿Qué es Blockchain y cómo funciona?

También conocido como cadena de bloques, blockchain es un tipo de ledger (*libro de registros*) que se distribuye para mantener un registro permanente, uno donde nadie puede manipular datos de transacción, pero cuando se debe alterar algo legítimamente, en un instante, toda la información en cada dispositivo se sincroniza, esto es posible porque la red de la cadena de bloques es peer to peer (p2p).

**Criptografía y Seguridad.**

Blockchain elimina los riesgos que conllevan los datos almacenados centralmente debido a que estos son distribuidos. Los métodos de seguridad de Blockchain son tecnología de cifrado. La seguridad contiene funciones digestivas, también llamadas funciones hash, las cuales transforman la información a un elemento de tamaño fijo y con ciertas características, lo cual permite crear un "ADN" único para la información registrada, permitiendo así que sea inmutable.

**Irreversibilidad.**

Al hablar de transacciones Bitcoin, una de las características del sistema Blockchain es que no permite anular transacciones directamente, a menos que todos los involucrados estén de acuerdo con la anulación o ya sea que el comerciante realice una transacción como devolución o anulación de una compra, pero eliminarla como tal del libro de registros es imposible.

**Descentralización y velocidad de respuesta.**

Blockchain desarrolla un sistema descentralizado totalmente seguro de toda la información que maneja. Esto es lo que hace que la información en los blockchain sea permanente, al tener todos, una copia de información, lo que hace que sea un sistema distribuido. Falsificar información es imposible debido a que no se puede modificar ni borrar nada, solo añadir; todo bajo un consenso.

**Estructura de los bloques.**

Un libro de registros consta de dos tipos de registros; las transacciones individuales y los bloques. El primer bloque se compone de un encabezado y datos pertenecientes a las transacciones permitidas en un tiempo establecido, el cual se utiliza para crear una cadena hash. Cada bloque que forma parte de la cadena está formado por un código hash que enlaza con el bloque anterior, el paquete de transacciones que incluye y otro código hash que enlaza con el siguiente bloque.

**Generación de claves.**

Para no depender sistema de usuario/contraseña para proteger nuestro perfil en línea, la seguridad de blockchain utiliza métodos de encriptación. La base del método son las claves públicas y privadas. Una clave pública, la cual es una larga cadena de números generada al azar, es la dirección de un usuario en el blockchain. La clave privada le da acceso al propietario acceso a archivos digitales que se encuentren en el blockchain y la información que se almacena es incorruptible. La red puede verificar que una transacción fue enviada por una que tenga la clave privada sin que esta revele su identidad.

**Mecanismo de replicación.**

El blockchain funciona como una red p2p, estas redes son un conjunto de ordenadores conectados entre sí, formando así “nodos”, donde se permite el intercambio directo de información, sin necesidad de acceder a un servidor central. Cada usuario que forma parte de cadena tendrá una copia completa y actualizada de la información.

**Arquitectura necesaria.**

La arquitectura necesaria para que el blockchain función es tener la plataforma de blockchain, nodos en la cadena de bloques, transacciones que forman parte de los bloques y el proceso de agregar bloques nuevos a la cadena. Esto se puede resumir en tres partes; la clave privada de criptografía (identidad), una red peer to peer (sistema de registro), y el programa (el protocolo de blockchain).

## Aplicaciones de Blockchain

El campo para la aplicación de blockchain es extenso debido al sistema que este sigue. Puede ser utilizado en campos tales como las fnanzas, el internet de las cosas, música, gobierno, identidad, etc. A continuación, veremos a detalle los mencionados anteriormente:

- Finanzas: la forma más conocida para el uso de blockchain, las criptomonedas son monedas electrónicas que viven únicamente en una cadena de bloques. Entre estas se encuentran los bitcoins, litecoin, o peercoin.
- Música: a través de blockchain, la piratería de la música podría dejar de ser un problema. Protegiendo los derechos de autor de los artistas, la distribución de la música tendría etiquetas en tiempo real de lo que sea haga con los archivos. Los artistas recibirían su pago con moneda digital y se evitaría la piratería.
- Gobierno: a la hora de realizar votaciones electorales, al utilizar un sistema electrónico para emitir los votos y evitar que estos sean manipulados, se puede hacer uso de blockchain para que cada voto sea encriptado para que luego se tenga un conteo transparente.

### ¿Cómo realizar administración de activos con Blockchain?

El uso de blockchain en el mundo empresarial nos proporciona diversos beneficios en el sector financiero y gubernamental. Tal y como se mencionó anteriormente, el uso de blockchain para realizar administración de activos nos permite agilizar procesos haciendo que estos sean confiables, eficientes y sobre todo con transparencia, lo cual nos ayuda a evitar fraudes y corrupción que son problemas diarios en un país.

## ¿Cuál es el futuro de Blockchain como tecnología?

El uso de blockchain cada vez ha ido creciendo y todo eso es gracias a los beneficios que este provee; la seguridad, la transparencia, le eficiencia, la velocidad, el respaldo asegurado de la información, entre otras. Sin lugar a duda, en un futuro próximo, todo funcionara en base a blockchain por las razones mencionadas anteriormente y que todas las acciones giran en torno a la tecnología y al internet.

Herramientas de desarrollo para la tecnología blockchain

- Ethereum: “Es una blockchain o tecnología de contabilada ditribuida (DTL) con un lenguaje de programación Turing completo integrado, con una computadora blockchain, que permite que cualquiera pueda escribir contratos inteligentes y aplicaciones descentralizadas simplemente escribiendo la lógica en unas pocas líneas de código.” Recuperado de: https://www.criptonoticias.com/informacion/que-es-ethereum/
- Hyperledger Fabric: “Es un proyecto colaborativo de código abierto que busca avanzar en el desarrollo de la tecnología entre industrias.” Recuperado de: https://www.criptonoticias.com/adopcion/hyperledger-project-consorcio-codigo-abierto-blockchain-empresarial/
- R3 Corda: “Es el libro distribuido de registros que puede ser considerado una blockchain.” Recuperado de: https://www.criptonoticias.com/banca-seguros/corda-la-plataforma-de-r3-que-se-asemeja-muy-poco-a-la-blockchain/

Comparación de las tres herramientas en Tabla No. 1

## Conclusión

Considerada como la nueva web del futuro, 3.0., blockchain promete seguridad de la información, capaz de reconocer cuando alguien intente realizar un fraude, haciendo inaccesibles archivos a hackers y a la manipulación de los mismos, ofreciendo respaldo de todas las transacciones. Introduciendo un nivel de democracia y objetividad, haciendo que nadie tenga poder absoluto y ni que pueda mentir en la red, blockchain es la futura promesa de mayor seguridad de información y transacciones y que será la base de todos los servicios en línea capaz de ser implementado en varios campos para su aplicación.

# Referencias

https://www.nobbot.com/firmas/blockchain-descentralizacion-confianza/

https://blockgeeks.com/guides/what-is-blockchain-technology/

https://www.coindesk.com/information/what-is-blockchain-technology/

https://www.coindesk.com/information/what-is-ethereum/

https://searchdatacenter.techtarget.com/es/definicion/Blockchain

https://academy.bit2me.com/que-es-cadena-de-bloques-blockchain/

https://medium.com/@igmata/criptograf%C3%ADa-b%C3%A1sica-para-entender-la-tecnolog%C3%ADa-blockchain-eb94cdd64158

https://criptomonedas.org/la-irreversibilidad-de-las-transacciones-bitcoin/

https://miethereum.com/blockchain/#toc22

http://cryptoparaprincipiantes.org/arquitectura-blockchain.html#Arquitectura_Blockchain_Ejemplo

https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6

Tablas

Tabla 1

Comparación de las herramientas de desarrollo de Blockchain.

| Characteristic | Ethereum | Hyperledger Fabric | R3 Corda |
|---|---|---|---|
| Description of platform | – Generic blockchain platform | – Modular blockchain platform | – Specialized distributed ledger platform for financial industry |
| Governance | – Ethereum developers | – Linux Foundation | – R3 |
| Mode of operation | – Permissionless, public or private[4] | – Permissioned, private | – Permissioned, private |
| Consensus | – Mining based on proof-of-work (PoW)<br>– Ledger level | – Broad understanding of consensus that allows multiple approaches<br>– Transaction level | – Specific understanding of consensus (i.e., notary nodes)<br>– Transaction level |
| Smart contracts | – Smart contract code (e.g., Solidity) | – Smart contract code (e.g., Go, Java) | – Smart contract code (e.g., Kotlin, Java)<br>– Smart legal contract (legal prose) |
| Currency | – Ether<br>– Tokens via smart contract | – None<br>– Currency and tokens via chaincode | – None |

*Fuente*: https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6

Tabla 2

Arquitectura necesaria para la tecnología blockchain

| **Blockchains are built from 3 technologies** | | |
|---|---|---|
| **1. Private Key Cryptography** | **2. P2P Network** | **3. Program (the blockchain's protocol)** |
| **Cash vs. Plastic** | **Tree falls in a forest** | **Tragedy of the commons** |
| **Identity** | **System of Record** | **Platform** |

*Fuente*: https://www.coindesk.com/information/what-is-blockchain-technology/

Ilustraciones

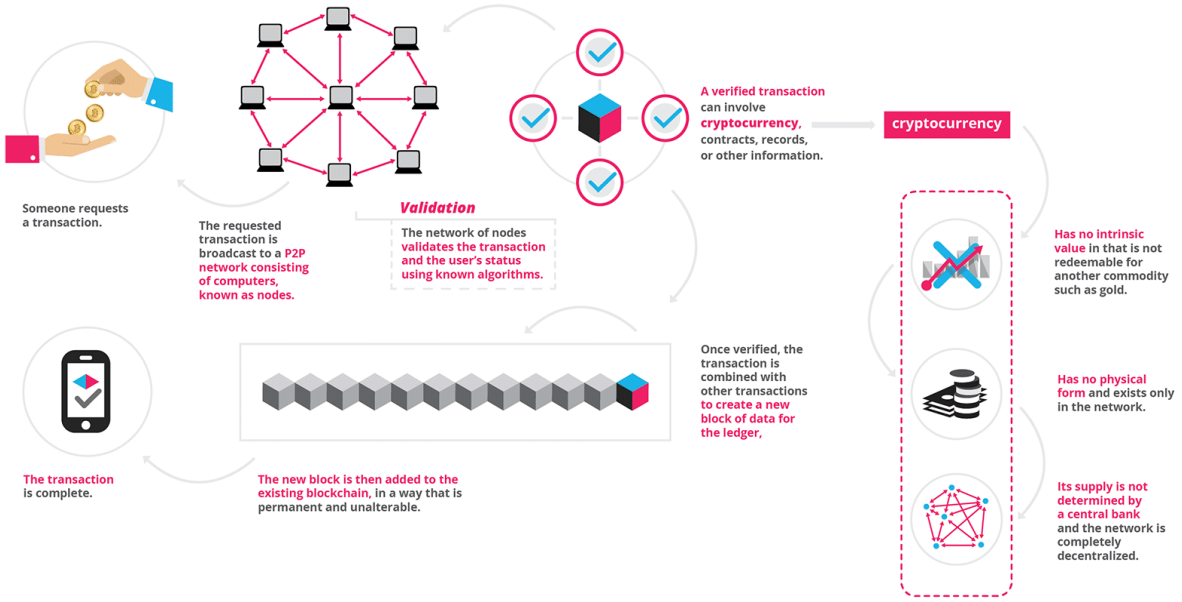


*Ilustración 1*. Proceso durante una transacción.

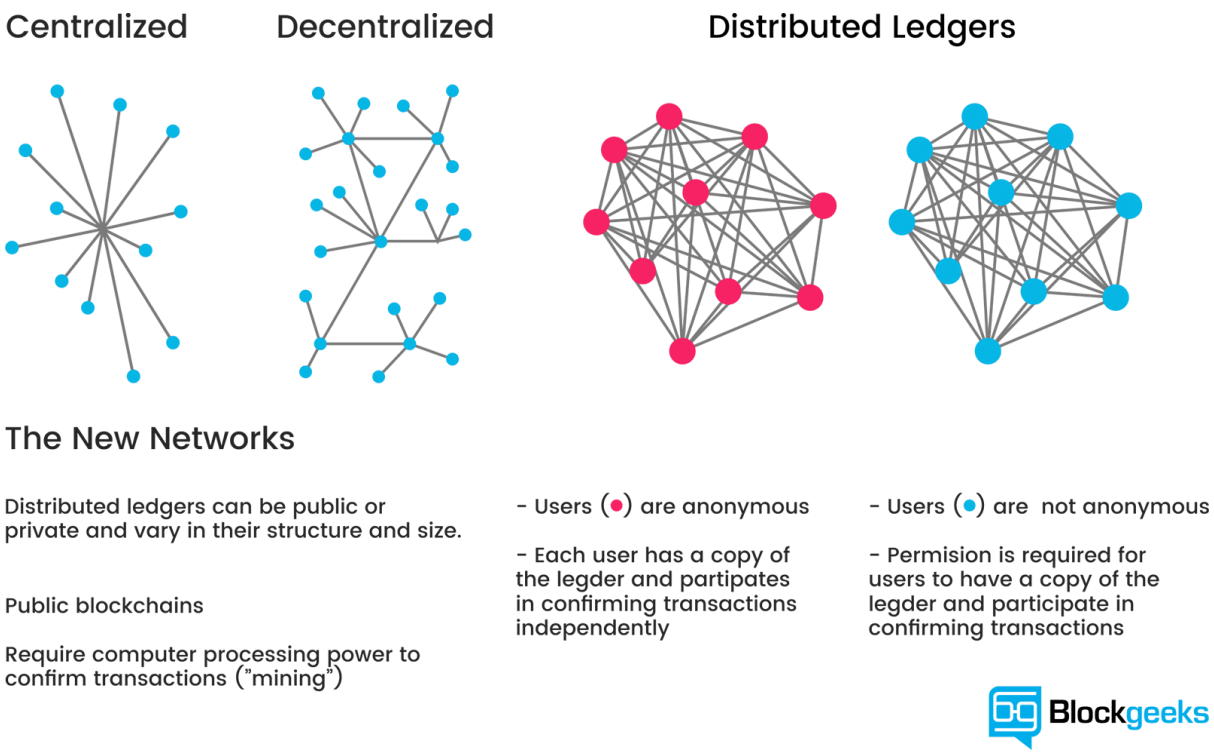


*Ilustración 2*. Tipos de redes de libros de registros.

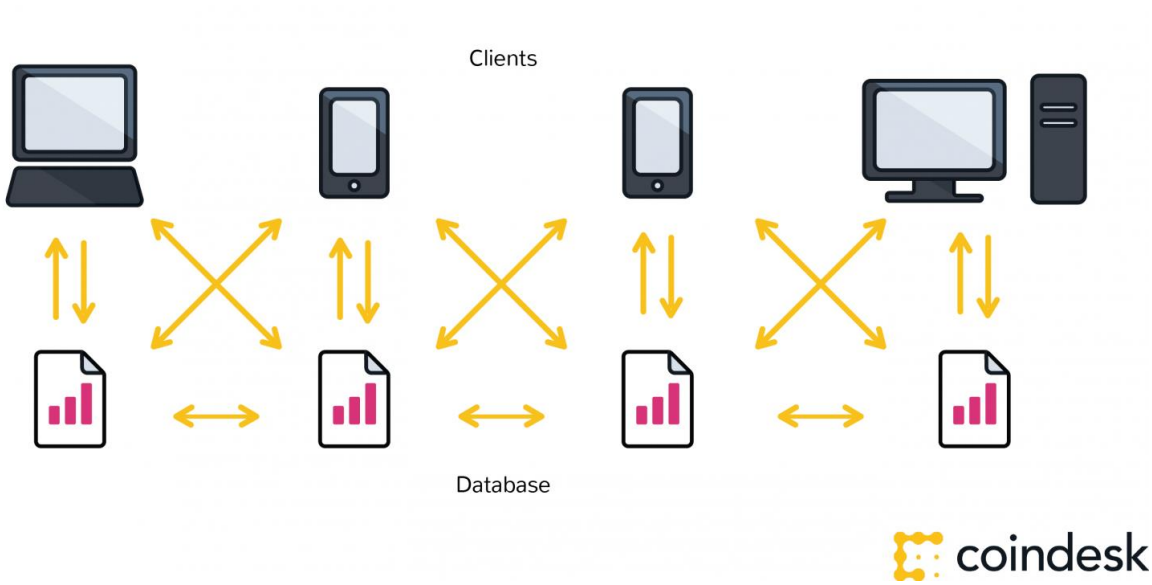


*Ilustración 3*. Representación del protocolo peer to peer (p2p).

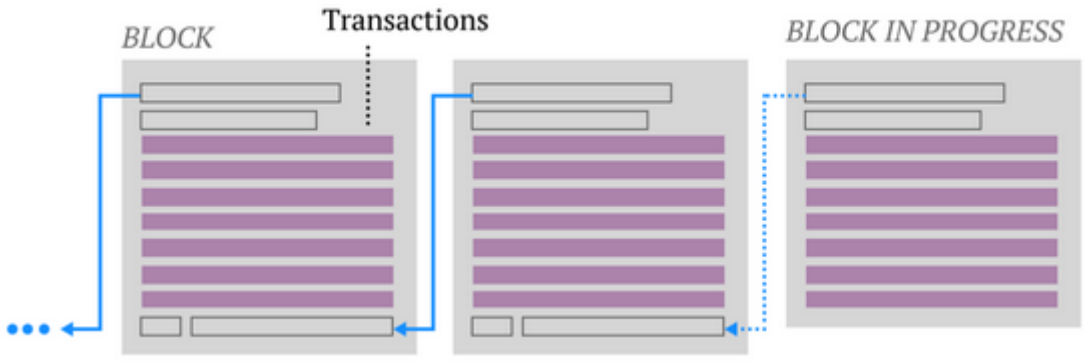


*Ilustración 4*. Estructura de los bloques

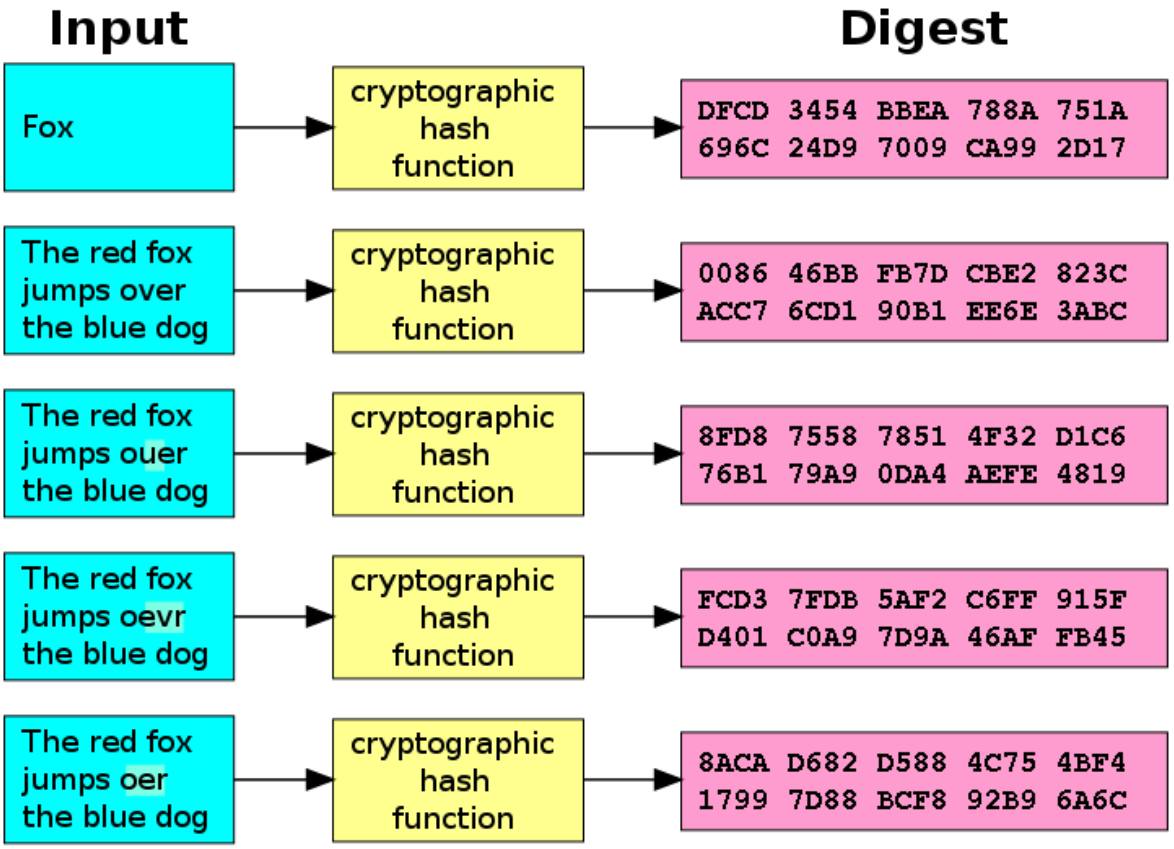


*Ilustración 4.* Funcion hash para encriptado.