# Definción de blockchain

Una blockchain es un tipo de base de datos especial. Es posible que hayas oído hablar también de la tecnología de registros distribuidos (distributed ledger technology o DLT) –en muchos casos, ambos conceptos se refieren a lo mismo.

Una blockchain presenta ciertas propiedades únicas. Existen reglas que determinan cómo deben ser añadidos los datos, y una vez éstos han sido almacenados, resulta virtualmente imposible modificarlos o eliminarlos.

Los datos se añaden, a lo largo del tiempo, en estructuras denominadas bloques.

# Bloques

Cada bloque se construye encima del anterior e incluye una porción de información que lo vincula a éste. Fijándonos en el bloque más reciente, podemos comprobar que ha sido creado después del anterior. Así que, si seguimos descendiendo por la “cadena”, llegaremos hasta nuestro primer bloque –conocido como bloque génesis.

Haciendo una analogía, imagínate que tienes una hoja de cálculo con dos columnas. En la primera celda de la primera columna, introduces cualquier información que desees conservar.

Los datos de esta primera celda serán convertidos en un identificador de dos letras, que se utilizarán a continuación como parte del siguiente input. En nuestro ejemplo, el identificador de dos letras KP deberá usarse para rellenar la siguiente celda en la segunda fila (defKP). Esto significa que si modificas los datos del primer input (abcAA), tendrás una combinación de letras diferente en todas las celdas restantes.



*Una base de datos en la que cada entrada está vinculada a la última.*

Si nos fijamos ahora en la fila 4, vemos que nuestro identificador más reciente es TH. ¿Recuerdas que comentábamos que no puedes volver atrás y eliminar o borrar entradas? El motivo es que sería fácil para cualquiera darse cuenta de que eso ha ocurrido, y tu tentativa de cambio simplemente sería ignorada.

Imagínate que cambias los datos de la primera celda –obtendrías un identificador distinto, lo que significa que tu segundo bloque tendría otros datos, dando lugar a un identificador diferente en la fila 2, y así sucesivamente. TH es, en esencia, un producto de toda la información que le antecede.

## ¿Cómo se conectan los bloques?

La discusión anterior –con nuestros identificadores de dos letras– es una analogía simple de la forma en que una blockchain emplea las funciones hash. El hashing es el pegamento que mantiene unidos los bloques. Consiste en tomar datos de cualquier tamaño para producir un output (un hash) que siempre presentará la misma longitud.

Los hashes utilizados en las blockchains resultan interesantes, debido a que la probabilidad de encontrar dos fragmentos de información que generen exactamente el mismo output, son astronómicamente bajas. Como con nuestros identificadores de arriba, cualquier ligera modificación de nuestros datos de input dará como resultado un output totalmente diferente.

Podemos ilustrarlo con SHA256, una función utilizada de forma extensiva en Bitcoin. Como puedes ver, incluso el empleo diferencial de mayúsculas basta para alterar por completo el output.

El hecho de que no se conozca la existencia de "colisiones" (es decir, dos inputs diferentes que den el mismo output) para SHA256, es increíblemente valioso en el contexto de las blockchains. Significa que cada bloque puede apuntar al que le antecede mediante la inclusión de su hash, y que cualquier intento de editar bloques viejos resultará evidente de forma inmediata.

# Blockchains y Descentralización

Hemos explicado la estructura básica de una blockchain. Pero cuando escuchas a la gente hablar de tecnología blockchain, probablemente no estén refiriéndose a la base de datos en sí misma, sino al ecosistema construido en torno a ella.

Como estructuras de datos independientes, las blockchains solamente son útiles para aplicaciones muy concretas. Donde la cosa se pone interesante es cuando las utilizamos como herramienta para que extraños se coordinen entre sí. En combinación con otras tecnologías y algo de teoría de juegos, una blockchain puede actuar como un libro mayor distribuido que no controla nadie.

Lo que esto significa es que ningún actor tiene el poder para editar las entradas saltándose las reglas del sistema (hablaremos más sobre las reglas en breve). En este sentido, podríamos argumentar que todo el mundo está en posesión del "ledger" de manera simultánea: los participantes se ponen de acuerdo respecto a su apariencia en todo momento.

## ¿Porqué las blockchains necesitan estar descentralizadas?

Uno podría, por supuesto, operar una blockchain en solitario. Pero terminaría teniendo una base de datos torpe, en comparación con otras alternativas superiores. Y es que su auténtico potencial sólo puede ser aprovechado en un entorno descentralizado –es decir, uno en el que haya igualdad entre todos los usuarios. De esta forma, la blockchain no podrá ser eliminada o maliciosamente dominada. Será una fuente de verdad única que estará a la vista de todos.

## ¿Qué es la red peer-to-peer?

La red peer-to-peer (P2P) es nuestra capa de usuarios (o la de los generales, en nuestro ejemplo previo). No hay un administrador, así que en lugar de conectar con un servidor central cada vez que alguien quiere intercambiar información con otro usuario, lo que hacen éstos es enviarla directamente a sus pares.

Fijémonos en el gráfico de abajo. A la izquierda, A necesita enviar su mensaje a través del servidor para hacérselo llegar a F. En el lado derecho, sin embargo, ambos están conectados sin un intermediario.

# ¿Qué son los contratos inteligentes?

El término Smart Contract o contrato inteligente se refiere a una pieza de código -software-, que se encarga de hacer cumplir un trato bajo ciertas condiciones, es similar a lo que sería un contrato físico en papel.

Un contrato inteligente trae múltiples beneficios, como: reducción de costos, mayor credibilidad ante ciertos contratos y descentralización en la toma de decisiones con respecto a qué debe hacer o no el contrato y la ejecución de este, esto último al no haber un humano interviniendo en el proceso de ejecución del contrato, lo que hace que sea a prueba de muchos fallos humanos causados por la interpretación errada del contrato o corrupción.

Cabe destacar que un humano debe intervenir en la creación del contrato así que en ese paso podrían omitirse algunos errores a la hora de codificar el contrato, causando que un contrato inteligente falle si el código no se hace de manera correcta.

# ¿Qué son las dApps?

Son aplicaciones descentralizadas que utilizan ‘blockchain’ para que los usuarios se relacionen directamente entre ellos y cierren acuerdos, sin que exista una entidad central que gestione el servicio.

# ¿Cómo funcionan?

A grandes rasgos, cada uno de los usuarios de una misma ÐApp es un nodo de una red descentralizada en la que todos los miembros actúan conjuntamente como un notario colectivo de cualquier movimiento que se realiza en esa plataforma. En la práctica, nadie debe dar su consentimiento de forma expresa, sino que todo funciona de manera automática y el propio sistema se encarga de corroborar la validez de cada interacción a través de un contrato inteligente, es decir, un programa informático que se ejecuta a sí mismo cuando se cumplen las condiciones programadas en su código. Cada vez que hay una nueva operación, la información de la plataforma se actualiza en cada nodo, donde queda almacenada una copia de todo el histórico de la ÐApp, así que cada usuario contribuye a mantener en pie la aplicación con los recursos de su ordenador.

Además, ese carácter distribuido propio de una cadena de bloques garantiza que en el caso de que desaparezca un nodo, existen otras muchas “copias de seguridad”. Esto acarrea lo que algunos expertos ven como el principal punto negativo de las ÐApps: almacenar una gran cantidad de datos en una cadena de bloques puede resultar costoso y aumenta de forma notable el tamaño de la misma en megabytes, aunque ya se está trabajando para mejorar este proceso y encontrar soluciones escalables.

# Ventajas

Como contrapartida, las aplicaciones descentralizadas presentan las siguientes ventajas con respecto a las “apps” tradicionales:

* La encriptación propia de una cadena de bloques proporciona una gran seguridad. Gracias a ello, la información sensible de los usuarios (como los datos fiscales o el historial médico) se blinda frente a robos, manipulación o ataques informáticos por parte de terceros, ya que no existe de forma centralizada en ninguna base de datos.
* La información publicada en redes sociales en formato ÐApp no podrá ser rastreada por ninguna entidad central para conocer los gustos o preferencias de los usuarios. Por lo tanto, se imposibilita la utilización de los datos personales con fines comerciales. De igual modo, en este tipo de aplicaciones desaparece la censura por parte de un administrador central.
* En lo referente a la prestación de servicios y alquiler de bienes muebles e inmuebles, las partes implicadas pueden cerrar acuerdos a través de contratos inteligentes o 'smart contracts' que se ejecutan de manera automática al cumplir ciertas condiciones. Por ejemplo, cuando alguien devuelve un coche alquilado, al momento recibe en su cuenta la fianza que adelantó por este servicio.
* No existen caídas del servicio porque todo está distribuido en nodos, no en unos servidores centrales, así que, si alguna de las partes de la red se cae, el resto sigue funcionando.

# Ejemplos de DApps

1. IDEX
2. ForkDelta
3. CryptoKitties
4. LocalEthereum
5. Bancor
6. Kyber Network
7. Decentraland
8. Ox
9. WINGS DAO
10. Etheroll

# Definición Bitcoin

Bitcoin es una moneda virtual o un medio de intercambio electrónico que sirve para adquirir productos y servicios como cualquier otra moneda.

Pero esta moneda es descentralizada, es decir que no existe una autoridad o ente de control que sea responsable de su emisión y registro de sus movimientos.

Consiste en una clave criptográfica que se asocia a un monedero virtual, el cual descuenta y recibe pagos.

# Sitiografía

[¿Qué es la Tecnología Blockchain? Guía Definitiva | Binance Academy](https://academy.binance.com/es/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners?utm_source=googleadwords_int&utm_medium=cpc&ref=HDYAHEES&gclid=CjwKCAiA0cyfBhBREiwAAtStHBa-4wZUDafqoPWW-d_ZWisrKEmpxoVWBO6YngCmz6h8xgToq6MxCxoCHywQAvD_BwE)

[Qué son las ÐApps y por qué serán cada vez más importantes (bbva.com)](https://www.bbva.com/es/que-son-las-dapps-y-por-que-seran-cada-vez-mas-importantes/)

[Ethereum DApps | 10 DApp principales de Ethereum | IG España](https://www.ig.com/es/estrategias-de-trading/las-10-dapp-principales-de-ethereum-201113)

[Especial Bitcoin: ¿qué es Bitcoin? ¿cómo funciona esta moneda virtual? (dinero.com)](https://especiales.dinero.com/bitcoin/index.html)