CURSO
Introducción a Blockchain

MÓDULO 1
“Descubriendo la tecnología DLT”

Contenido

1. OBJETIVOS DEL MÓDULO

En este módulo aprenderemos sobre:

- Tecnologías de Registro Distribuido (DLT)
- Blockchain y sus características
- Blockchain permisionadas vs blockchain no permisionadas
- Algoritmos de consenso y smart contracts

2. INTRODUCCIÓN

La tecnología blockchain se conoció gracias a Satoshi Nakamoto quien introdujo Bitcoin en el mercado allá por el año 2009, mostrando cómo se utilizaba esta nueva tecnología descentralizada.

Bitcoin es una blockchain pública. Cualquiera puede unirse a la red y usarla sin restricciones.

Poco después del surgimiento de Bitcoin, nació en 2015 una nueva blockchain pública Ethereum, la cual prosperó en el mercado. Se hizo muy popular rápidamente sobre todo por haber incorporado el concepto de "contratos inteligentes".

Cuando surgieron estas "criptomonedas", los empresarios y tecnólogos aumentaron su interés sobre la tecnología blockchain pero enfocando su interés a la creación de blockchain privadas que den solución a un sin fin de problemas.

RECORDAR: **Blockchain no es Bitcoin**. Bitcoin y las criptomonedas son excelentes casos de uso para blockchain pero hay muchos casos de uso que utilizan esta tecnología.

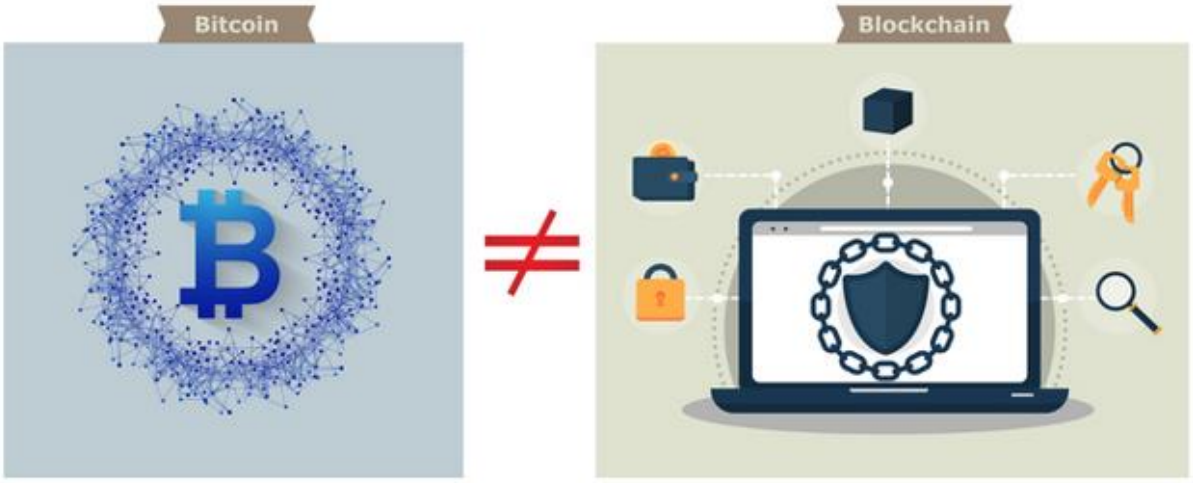

Fig. 1 Hablar de Bitcoin es distinto a hablar de Blockchain.

Blockchain forma parte de las Tecnologías de Registro Distribuido, sobre la cual hablaremos a continuación.

3. TECNOLOGÍA DE REGISTRO DISTRIBUIDO

Para introducirnos en el concepto de Distributed Ledger Technologies (DLT) o Tecnología de Registro Distribuido en su traducción al español, es necesario pensar en el concepto de Base de Datos.

Para quienes no conocen este término, una base de datos no es nada más que un conjunto de datos organizados, con cierta estructura, que poseen relaciones entre sí.

Las bases de datos con las que trabajamos a diario normalmente se encuentran almacenadas en un único repositorio físico, al que podemos acceder cuando ingresamos a un sistema, plataforma o aplicación.

De esta manera, los datos se encuentran en un solo lugar y debemos confiar en que son veraces y que no han sido alterados.

Ahora bien, DLT nos propone el uso de blockchain que puede definirse como una especie de base de datos que se encuentra almacenada en el ordenador o computadora de quien la utiliza.

De esta manera cada vez que alguien agrega un dato a la blockchain, este dato será enviado a todos los usuarios para que agreguen un bloque de información en la blockchain que poseen.

A los fines de este curso se utilizará indistintamente la denominación **Tecnología de Registro Distribuido** o **Tecnología de Libro Mayor Distribuido**.

Un Registro Distribuido es un tipo de estructura de datos que reside en múltiples dispositivos informáticos, generalmente distribuidos en ubicaciones o regiones. La tecnología de Registro Distribuido incluye tecnologías de blockchain y contratos inteligentes.

Mientras que los registros distribuidos existían antes de Bitcoin, como lo mencionamos anteriormente, la cadena de bloques de Bitcoin marca la convergencia de una gran cantidad de tecnologías, incluida la marca de tiempo de las transacciones, las redes Peer-to-Peer (P2P), la criptografía y el poder computacional compartido, junto con un nuevo algoritmo de consenso.

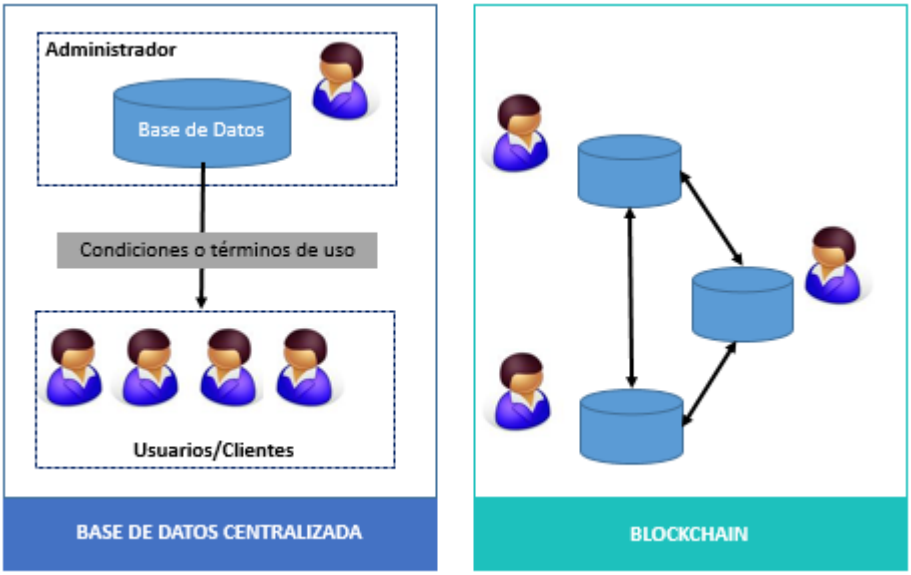

Fig. 2 Bases de Datos vs Blockchain

3.1 Componentes Básicos

La tecnología de registro distribuido generalmente consta de tres componentes básicos:

- Un modelo de datos que captura el estado actual del registro.
- Un lenguaje de transacciones que cambia el estado del libro mayor o registro.
- Un protocolo utilizado para generar consenso entre los participantes acerca de qué transacciones se aceptarán y en qué orden.
- A lo largo del curso profundizaremos cada uno de estos conceptos.

3.2 Concepto de Blockchain

3.2.1 Concepto I

Tal como lo mencionamos en la introducción de este módulo, **Blockchain** es una forma o subconjunto específico de Tecnología de Registro Distribuido, que construye una cadena cronológica de bloques (blocks), de ahí el nombre de "cadena de bloques".

Un **bloque** se refiere a un conjunto de transacciones que se agrupan y agregan a la cadena al mismo tiempo.

Veamos una analogía. Un bloque en una cadena de bloques puede considerarse como una página en un cuaderno. Los datos se almacenan en un bloque, al igual que los datos se escriben en una página de un cuaderno.

3.2.2 Concepto II

La **marca de tiempo** es otra característica clave de la tecnología blockchain. Cada bloque tiene la marca de tiempo y cada nuevo bloque hace referencia al bloque anterior. Combinado con hashes criptográficos[1], esta cadena de bloques con marca de tiempo proporciona **un registro inmutable** de todas las transacciones en la red, desde el primer bloque.

El primer bloque de cualquier blockchain se conoce como el bloque génesis. Solo el bloque génesis no tiene ningún bloque precedente.

En la cadena de bloques de Bitcoin, los nodos mineros agrupan transacciones no confirmadas y válidas en un bloque. Cada bloque contiene un número dado de transacciones. En la red de Bitcoin, los mineros deben resolver un desafío criptográfico para proponer el siguiente bloque. Este proceso se conoce como "prueba de trabajo" (o *Proof of Work -PoW*) y requiere una gran capacidad de cálculo.

Un bloque comúnmente **consiste en** cuatro piezas de metadatos:

- La referencia al bloque anterior.
- La prueba de trabajo
- La marca de tiempo
- La raíz del árbol Merkle para las transacciones incluidas en este bloque

3.2.3 Concepto III

Almacenamiento de datos y encadenamiento de Bloques:

Cualquier dato puede almacenarse en el mismo bloque. Algunos ejemplos de datos almacenados incluyen:

- Registros médicos
- Acuerdos sobre propiedades
- Voto

[1] Hash: cadena alfanumérica de longitud fija usada para cifrar datos.

Cada bloque está encadenado o atado al bloque anterior mediante información del bloque anterior embebida en el bloque actual. Más adelante veremos cómo se logra.

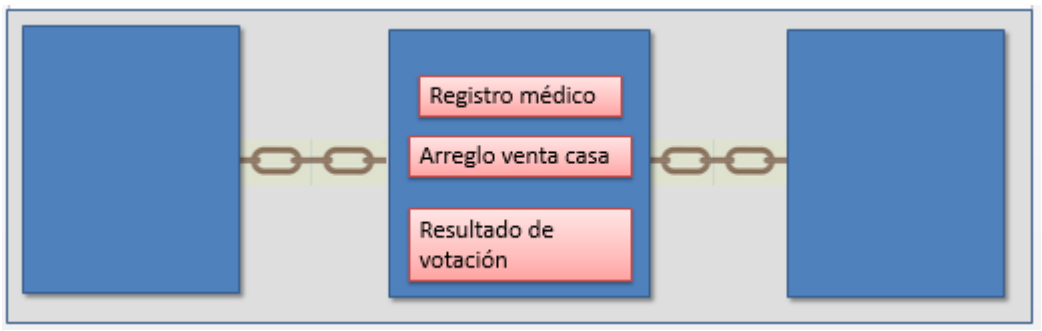

Fig. 3 Ejemplo de bloques encadenados.

Árbol de Merkle

El árbol de Merkle es una estructura de datos que se utiliza para almacenar los hashes de los datos individuales en grandes conjuntos de datos, de manera que la verificación del conjunto de datos sea eficiente. También es conocido como árbol de hash binario. Es un mecanismo anti sabotaje para garantizar que el gran conjunto de datos no se haya modificado. La palabra 'árbol', en informática, se usa para referirse a una estructura de datos ramificada como se ve en la imagen a continuación.

El término *hash* se refiere a un código generado para el bloque anterior mientras que *nonce* es el término utilizado para hacer referencia a un número arbitrario único.

Según Andreas M. Antonopoulos[2], en el protocolo Bitcoin: "Los árboles de Merkle se utilizan para resumir todas las transacciones en un bloque, produciendo una huella digital global de todo el conjunto de transacciones, proporcionando un proceso muy eficiente para verificar si una transacción está incluida en un bloque".

[2] https://es.wikipedia.org/wiki/Andreas_Antonopoulos

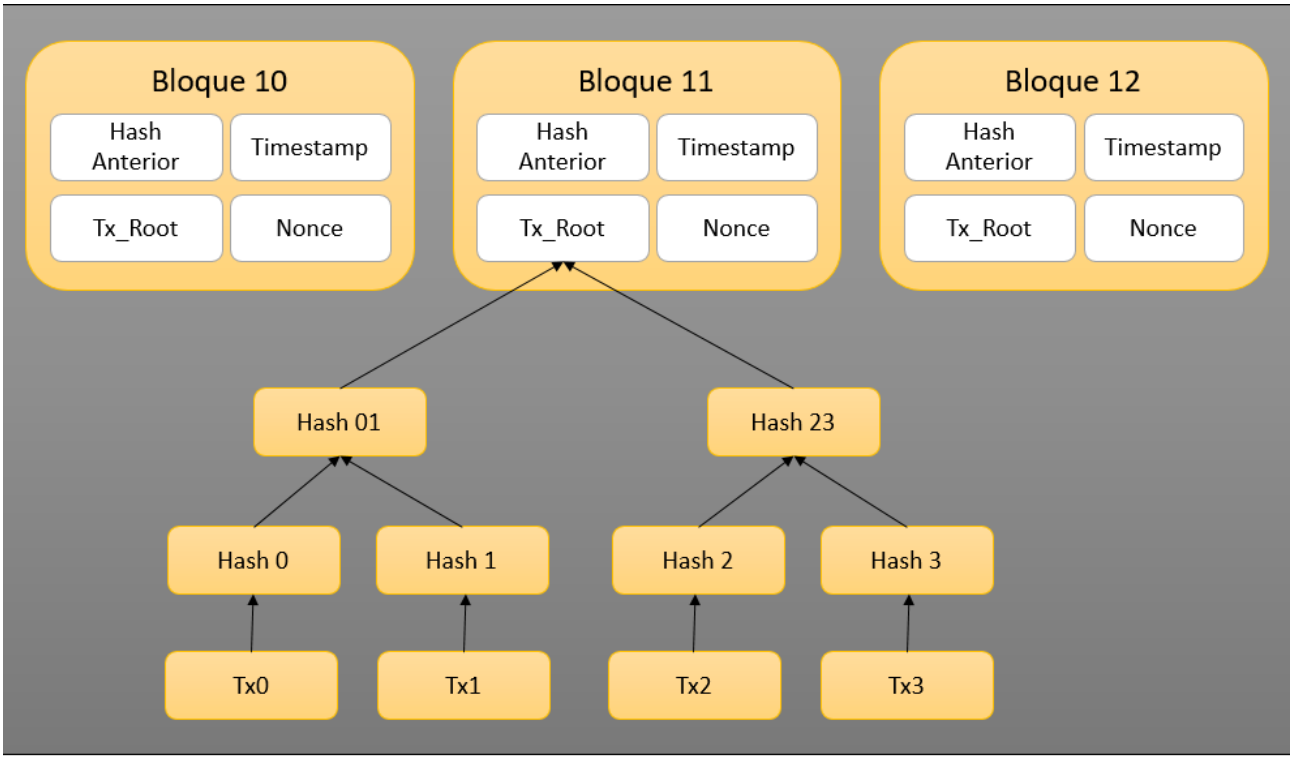

Fig. 4 Árbol de Merkle

3.3 Criptografía de Clave Pública

La criptografía de clave pública utiliza un par de clave pública y una clave privada para realizar diferentes tareas. Las claves públicas se distribuyen ampliamente, mientras que las claves privadas se mantienen en secreto.

Al usar la clave pública de una persona, es posible cifrar un mensaje para que solo la persona con la clave privada pueda descifrarlo y leerlo. Usando una clave privada, se puede crear una firma digital para que cualquier persona con la clave pública correspondiente pueda verificar que el mensaje fue creado por el propietario de la clave privada y no se modificó desde entonces.

Blockchain hace un amplio uso de la criptografía de clave pública.

Fig. 5 Clave pública y clave privada.

3.4 Blockchain Características

Consenso: para que una transacción sea válida, todos los participantes deben estar de acuerdo con su validez.

Procedencia: los participantes saben de dónde provino el activo y cómo ha cambiado con el tiempo.

Inmutabilidad: ningún participante puede manipular una transacción una vez que se haya registrado en el libro. Si una transacción es errónea, se debe usar una nueva para revertir el error, y ambas transacciones son visibles.

Finalidad: un único registro compartido proporciona un lugar al que se puede acceder para determinar la propiedad de un activo o la finalización de una transacción.

3.5 Conceptos Clave

Para poder comprender el funcionamiento de blockchain es necesario introducirnos en algunos conceptos clave:

Registro Compartido: Sistema de Registro Distribuido de solo "anexos" compartido a través de la red de negocios o red empresarial.

Permisos: al asegurar una apropiada visualización, las transacciones son seguras, autenticadas y verificables.

Smart Contract: los términos o condiciones de trabajo integrados en la base de datos de las transacciones y ejecutados con las transacciones.

Minería: la generación de bloques es un proceso proporcionado, en el caso de las redes públicas, por la minería. Esto requiere de un alto costo computacional para poder validar un bloque.

Consenso: es un método mediante el cual se validan las transacciones. Todas las partes (nodos) de la red acuerdan las reglas de negocio y aceptan la transacción verificada.

3.6 Tipos de Arquitecturas

Blockchain Tipos de Arquitecturas I

Las cadenas de bloque se clasifican de acuerdo a los permisos que otorgan. En este sentido una blockchain puede ser no permisionada (como Bitcoin o Ethereum) o permisionada (como los diferentes *frameworks* de blockchain de Hyperledger).

Una blockchain no permisionada también se conoce como una cadena de bloques pública, porque cualquiera puede unirse a la red.

Una blockchain autorizada, o blockchain permisionada, requiere una verificación previa de las partes participantes dentro de la red, y estas partes generalmente se conocen entre sí.

Las blockchain federadas o de consorcio es el último tipo de arquitectura que ha surgido, tomando lo mejor de la arquitectura de blockchain pública y lo mejor de la arquitectura de blockchain privada.

Blockchain Tipos de Arquitecturas II

Las blockchain permisionadas deben ser impulsadas por la aplicación particular que se quiera realizar. La mayoría de los casos de uso empresariales implican una negociación exhaustiva antes de que las partes acuerden hacer negocios entre sí.

En la tabla a continuación extraída de la web de 101Blockchains [3]se puede ver una comparación entre los tres tipos de arquitecturas descriptas.

[3] https://101blockchains.com/es/

Características	Blockchain Privada	Blockchain Pública	Blockchain Federada
Acceso	Privada	Pública	Público/Privada
Consenso	Basada en la organización	Pública	Nodos seleccionados
Eficiencia	Alta	Baja	Alta
Centralización	Si	No	Parcial
Proceso de Consenso	Basada en permisos	Basada en permisos	Sin permiso
Inmutabilidad	No completamente a prueba de manipulaciones	Completamente a prueba de manipulaciones	No completamente a prueba de manipulaciones

Fig. 6 Blockchain privada vs. blockchain pública.

3.7 Participantes y Roles

La construcción y futura operación de una blockchain, requerirá de distintos participantes y roles, que se detallan a continuación:

Usuarios de la blockchain: un participante (usuario del negocio) con permisos para unirse a la blockchain y llevar a cabo transacciones con otros participantes de la red. Estos serán múltiples usuarios interactuando sobre una capa de negocios. La blockchain se ejecuta por detrás, es transparente para ellos pero les da la fiabilidad necesaria para negociar.

Regulador: es un tipo de usuario especial con permisos para observar las transacciones que ocurren en la red. Se puede prohibir a los reguladores realizar transacciones.

Desarrollador de la Blockchain: son los programadores que crean las aplicaciones y los smart contracts para que los usuarios de la blockchain puedan ejecutar sus transacciones.

Operador de la Red Blockchain: individuos que tienen permisos y autorización especial para definir, crear y manejar la red blockchain. Cada negocio sobre blockchain tendrá un operador de red.

Plataformas de Procesamiento Tradicionales: sistemas de computadora existentes que podrán ser usadas por la blockchain para aumentar el procesamiento.

Fuentes de dato Tradicionales: son los sistemas de datos existentes que proveerán datos para la ejecución de los smart contracts.

Autoridad Certificante: un individuo que gestiona los diferentes tipos de certificados requeridos para ejecutar la blockchain permisionadas.

> Cuando hablamos de red empresarial o red de negocios, hacemos referencia a TODOS los participantes de la blockchain.

3.8 Algoritmo de Consenso

El consenso en la red se refiere al proceso de lograr un acuerdo entre los participantes de la red en cuanto al estado correcto de los datos del sistema.

El consenso hace que todos los nodos compartan exactamente los mismos datos. Por lo tanto, un algoritmo de consenso hace dos cosas: garantiza que los datos en el registro sean los mismos para todos los nodos de la red y, a su vez, evita que los actores malintencionados manipulen los datos. El algoritmo de consenso varía según la implementación de blockchain.

3.8.1 Proof of Work

El algoritmo de consenso Proof of Work (PoW - Prueba de trabajo) es el usado por Bitcoin. Implica resolver un "rompecabezas computacional" desafiante para crear nuevos bloques en la cadena de bloques.

Coloquialmente, el proceso se conoce como "minería" y los nodos de la red que participan en la minería se conocen como "mineros". El incentivo para las transacciones mineras radica en los beneficios económicos, donde los mineros que compiten son recompensados con 12.5 bitcoins y una pequeña tarifa por transacción.

"La prueba de trabajo (PoW) es el resultado de un proceso minero exitoso y, aunque la prueba es difícil de crear, es fácil de verificar", Informe de seguridad 2016 de Kudelski[4].

Para una mejor comprensión, podemos considerar el siguiente ejemplo proporcionado por Ofir Beigel: "(...) adivinar una combinación a un candado es un gran desafío. Es muy difícil conseguirlo, ya que deberemos realizar muchas combinaciones diferentes; pero una vez que se obtiene la correcta, es fácil de validar. Simplemente se ingresa la combinación y se comprueba que la cerradura abre".

Existen múltiples críticas para el algoritmo de consenso de PoW, especialmente por la gran cantidad de energía que necesita para ejecutar el algoritmo computacional. Por ende, la mayoría de las computadoras que realizan la minería se ubican en los países donde la electricidad es barata.

En términos de seguridad de la red, PoW es susceptible al "51% de ataque", lo que significa un mayor poder de minado por parte de una persona o grupo de mineros. En un escenario con actores

[4] https://www.kudelskisecurity.com/sites/default/files/files/kudelski_Security_blockchain_20161213.pdf

maliciosos, esto puede provocar que los atacantes no permitan realmente transferir dinero, iniciando una bifurcación en la cadena.

3.8.2 Proof of Stake

El algoritmo Proof of Stake (PoS - Prueba de Participación) es una generalización del algoritmo Proof of Work utilizada por Ethereum.

En PoS, los nodos se conocen como "validadores" y validan las transacciones para obtener una "tarifa" de transacción.

No hay que hacer minería, ya que todas las monedas existen desde el primer día.

En pocas palabras, los nodos se seleccionan al azar para validar bloques, y la probabilidad de esta selección aleatoria depende de la cantidad de participación retenida. Por lo tanto, si el nodo X posee 2 monedas y el nodo Y posee 1 moneda, el nodo X tiene el doble de probabilidades de ser llamado para validar un bloque de transacciones.

La implementación específica de PoS puede variar, dependiendo del caso de uso, o como una cuestión de diseño de software.

El algoritmo de PoS ahorra costosos recursos computacionales que se gastan en minería bajo un régimen de consenso de PoW.

3.8.3 Tolerancia a Fallas Bizantino

El algoritmo de consenso Tolerante a fallos bizantinos simplificado implementa una versión adoptada del algoritmo Práctico Tolerante a fallos bizantinos (PBFT), y busca proporcionar mejoras significativas sobre el protocolo de consenso de PoW de Bitcoin.

La idea básica involucra a un único validador que agrupa las transacciones propuestas y forma un nuevo bloque.

A diferencia de la cadena de bloques de Bitcoin, el validador es una parte conocida, dada la naturaleza autorizada del registro distribuido.

El consenso se logra como resultado de un número mínimo de otros nodos en la red que ratifican el nuevo bloque.

Para ser tolerante a una falla bizantina, el número de nodos que deben alcanzar el consenso es 2f + 1 en un sistema que contiene 3f + 1 nodos, donde f es la cantidad de fallas en el sistema. Por ejemplo, si tenemos 7 nodos en el sistema, entonces 5 de esos nodos deben estar de acuerdo si 2 de los nodos están actuando de manera defectuosa.

3.9 Smart Contract

Un smart contract es un arreglo o conjunto de reglas que gobiernan las transacciones de negocio. Estos son almacenados en la blockchain y se ejecutan de manera automática como parte de la transacción [Wiley & Sons, 2018[5]].

Por ejemplo, la compañía aérea *Volar* podría tener entre sus términos y condiciones una regla que se dispara automáticamente cuando el vuelo se demora más de seis horas y emite un crédito a favor del pasajero.

En pocas palabras, los smart contracts son programas de computadora que ejecutan acciones predefinidas cuando se cumplen ciertas condiciones dentro del sistema.

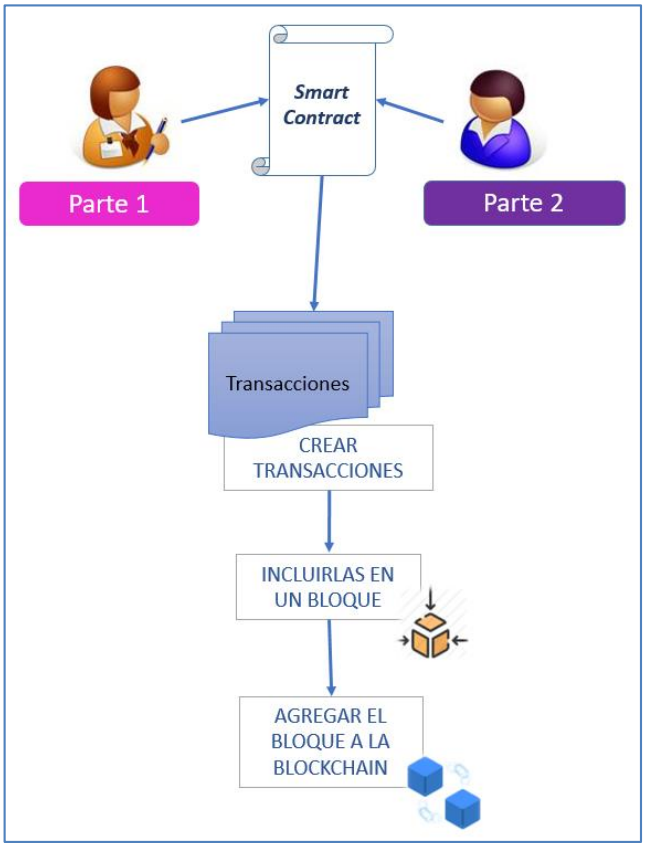

Fig. 7 Funcionamiento de los smart contract o contratos inteligentes.

3.10 ¿Cómo funciona Blockchain?

¿Cómo funciona Blockchain? I

Si bien el funcionamiento de una blockchain resulta un poco complejo a la hora de su implementación, entender su comportamiento conceptualmente es bastante sencillo.

[5] The bitcoin standard: the decentralized alternative to central banking. John Wiley & Sons, 2018.

Para eso vamos a tomar como ejemplo el caso de la cadena de suministro de hongos de pino de la Patagonia.

Definimos nuestros actores:

Juan: es un pequeño productor de hongos de pino de la Patagonia que abastece a restaurantes y hoteles de alta gama.

Regulador: es quien verifica que la actividad de Juan se realiza de forma legal cumpliendo con las regulaciones actuales (por ejemplo: el Registro Nacional de Certificadoras Orgánicas, dependiente del SENASA).

Flavia: es la dueña de uno de los hoteles boutique de la Patagonia, quien abastece al cliente final, en este escenario.

Fernando: es el dueño de un restaurante en el pueblo. Juan puede vender directamente los hongos a Fernando.

Todo el proceso productivo se encuentra certificado. El proceso de fabricación comienza con la siembra de semillas certificadas y finaliza con la cosecha y embalaje de los productos. Las cepas de cada variedad de hongo se compran a proveedores certificados. La venta se realiza de forma directa a restaurantes u hoteles dado que hay que optimizar el tiempo de cosecha y consumo. El costo de venta es de $100 (pesos cien) por kilo cosechado. Para poder llegar a más puntos estratégicos de consumo, Juan hace una degustación de productos y descuentos en la primera compra.

¿Cómo funciona Blockchain? II

Continuando con el escenario propuesto, Juan podrá escribir en la blockchain cada vez que realiza una cosecha.

El controlador podrá verificar los certificados del ciclo de siembra en la red.

Flavia podrá negociar con Juan el precio por 10 kg de hongos, mientras que Fernando realizará la compra de 2 kg para probar el producto. Ambas transacciones se reflejarán en la blockchain.

Transacciones:

1. Cargar cosecha, con fecha 20/Abril/2020 y detalle de semillas.

2. Compra de Flavia, 10 Kg a $800. Descuento por compra al por mayor.

3. Compra de Fernando, 2kg a $100, bonificado 1kg por ser cliente nuevo.

Cada una de las transacciones listadas, se registrarán en un bloque de la blockchain (ver imagen). Por lo tanto cada uno de los integrantes de la red de negocio, tendrá una copia del bloque generado.

BLOQUE
Timestamp
Hash anterior
Identificador_Cosecha
Identificador_Cosechador
N° certificado de semillas
Tipo de hongo
Kg cosechados
Fecha de cosecha
Nonce

Fig. 8 Bloque de ejemplo.

Si Juan actuase de forma maliciosa y pretendiese modificar el certificado de las semillas cosechadas al 20/Abril/2020, luego de haber generado el primer bloque, rápidamente los demás integrantes de la blockchain rechazarían la transacción, puesto que el hash del certificado de semillas cosechadas, no será el mismo.

Vamos a estudiar entonces qué es una función hash.

3.10.1 Función Hash

Cada bloque de la blockchain es un registro de información cifrada, cada uno encadenado al anterior con "criptografía". Esta característica es la que hace a la blockchain inmutable.

Una función hash criptográfica es un algoritmo que cuenta con ciertas propiedades para el cifrado de datos, es decir, para proteger contenido mediante el uso de claves. Hablamos de "contenido" dado que se puede obtener el *hash* tanto de un dato, un mensaje o texto como así también de una imagen, documento de texto o video.

Al aplicar la función hash, se cifra el contenido y se obtiene como resultado una cadena alfanumérica de longitud fija denominada hash, sin importar el tamaño del mensaje o contenido original. Por lo tanto, se usa para verificar que el contenido no ha sido modificado. Cualquier punto que se agregue a un mensaje por ejemplo, cambiaría el hash. Miremos la imagen a continuación:

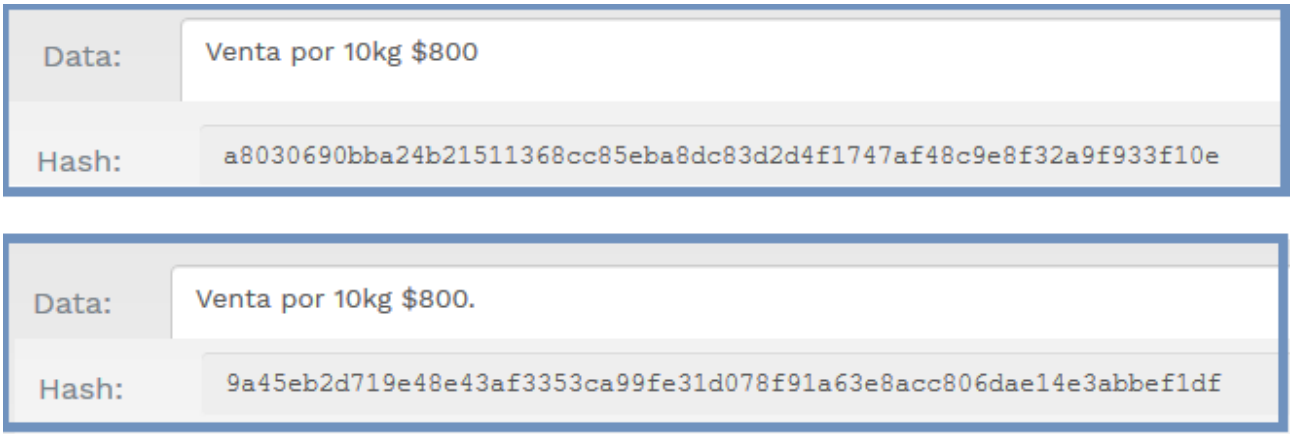

Fig. 9 Función hash.

Observen cómo al introducir el texto "Venta por 10kg $800" en una función *hash* se obtiene un código *hash* totalmente diferente al que se obtiene en la segunda parte de la imagen en donde solo se agregó un punto al final.

De la misma manera, cada bloque de información tendrá asociado un *hash*. Entonces por ejemplo, el bloque A posee el *hash 012YJ* que será almacenado en el bloque siguiente (bloque B) de forma tal que se conozca cuál es el bloque anterior.

Una mínima modificación sobre los datos o transacciones almacenadas en el bloque A, harán que se modifique el *hash*; supongamos que se transforma en 789XC. El nuevo *hash* es distinto al almacenado en su sucesor B.

En este ejemplo, queda a la vista que alguien ha intentado modificar de forma maliciosa la información almacenada en la blockchain. Cuando se intente transmitir este bloque de información con un hash diferente, el resto de los participantes se darán cuenta y rechazarán al bloque que intenta adjuntarse a la blockchain.

¿Cómo funciona Blockchain? III

Una vez aclarado el concepto de hash, vamos a continuar con el escenario del ejemplo para comprender un poco más acerca de transacciones y *smart contracts.*

En la imagen podemos ver a todos los actores de nuestro escenario: Juan: el agricultor, Flavia y Fernando: potenciales compradores, y el Regulador.

Juan podrá introducir en un bloque una transacción por ejemplo para informar sobre la cosecha del 20 de Abril. Los pares 1 y 2 (ver imagen) son quienes validan esa transacción y la agregan al bloque a la blockchain.

Tal como supusimos con anterioridad, Juan y Flavia realizan un acuerdo diferente al que se ejecuta entre Juan y Fernando. Cada uno de estos acuerdos se implementa como un smart contract diferente. De la misma manera la ejecución del smart contract dará como resultado un bloque con una transacción que será validada por alguno de los pares de acuerdo al método de consenso elegido.

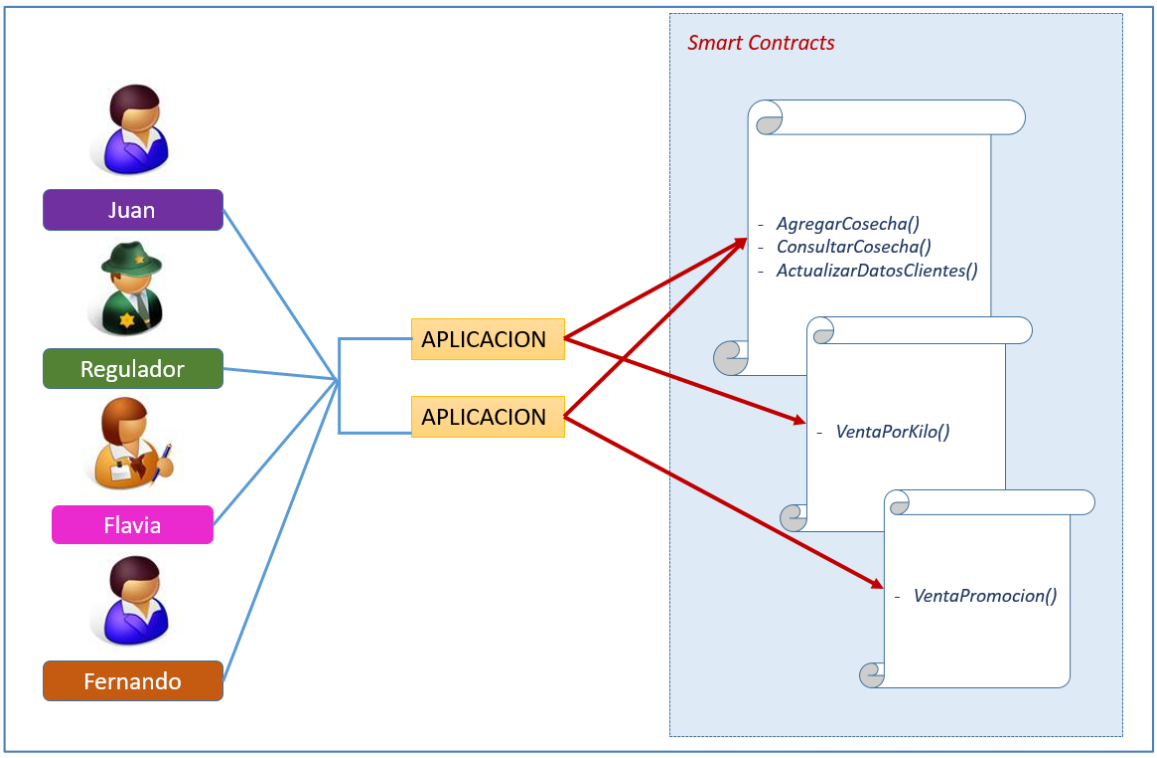

Fig. 10 Interacciones usando contratos inteligentes.

3.11 Arquitectura de una red DLT

Una red DLT se implementa sobre una estructura (arquitectura) que contiene diversos estratos, niveles o capas:

- Una primera llamada infraestructura (máquinas de computación y almacenaje de datos, y red de comunicación, que pueden ser servidos en la nube o mantenidos por cada nodo);
- Una segunda denominada plataforma (comunicación internodal, software de protocolo de consenso, servicios de encriptación de datos, firma digital y otros que aseguran la inmutabilidad del registro, y contratos inteligentes);
- Una tercera de interfaces de programación de aplicaciones (conocidos como API) útiles para conectar la plataforma con las aplicaciones externas a la red (que incluye los mecanismos de gestión nodal, uniforme, y los de descarga y acceso a datos registrados);
- Y una última, de aplicaciones descentralizadas (DApps) que contiene sistemas fuera de la red conectados a ésta: como oráculos para smart contracts, conexiones de IoT/AI y enlaces con sistemas empresariales y datos externos que permiten a los clientes interactuar con la red.

Es necesario advertir que la implementación de blockchain depende en su totalidad del tipo de arquitectura elegida, por lo tanto la herramienta con la que se desarrolle será distinta. En el módulo 3 profundizaremos en cómo se implementa una blockchain.

4. CONCLUSIONES DEL MÓDULO

En este primer módulo hemos presentado la tecnología DLT que abarca tanto a blockchain como a los smart contracts. Se han descripto los componentes básicos y las características que las hacen tan prometedoras.

Se abordó el estudio de los algoritmos de consenso más conocidos: PoW (Proof of Work) y PoS (Proof of Stake).

También revisamos cómo se genera un hash para poder hacer inmutable a un bloque de la cadena de bloques.

En el Módulo II vamos a analizar algunos casos de uso de blockchain en el mercado y en la Administración Pública Nacional.