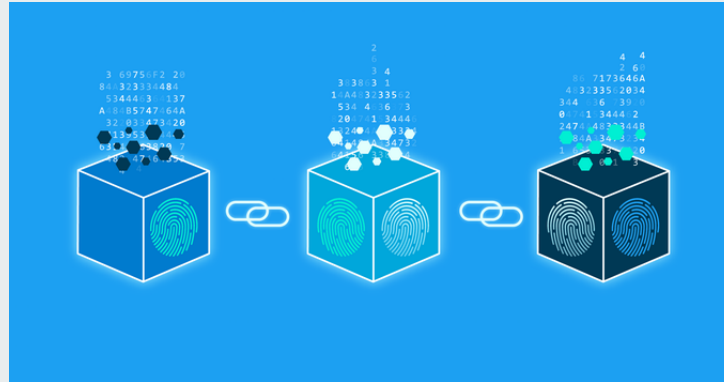


# Cloud Computing: Servicios y Aplicaciones



# Luis Gallego Quero

# Índice



1. ¿Qué es blockchain?
2. Componentes
3. Características y funcionamiento
4. Aplicaciones
5. Blockchain as a Service



# ¿Qué es blockchain?

Tuvo su origen para las transacciones con bitcoin, por lo que fue originalmente utilizada por figuras que se oponían al sistema establecido y que buscaban conseguir **independencia** sobre un control central.

# ¿Qué es blockchain?



## - Situación 1: Una **transacción monetaria**.

- Pagamos un dólar por algún bien material, pero esta transacción se realizó porque el valor de un dólar está representado por un billete, el cual fue creado por un gobierno en el que ambas partes confían, que se reconocen y aceptan. Entonces cuando esta compra-venta se concreta, los detalles deben quedar escritos en un libro de cuentas.

- Las transacciones electrónicas es similar, ya que entran en participación terceras partes fiables como bancos u operadores como Paypal.

## - Situación 2: **Moneda virtual**.

- Se garantiza la integridad y fiabilidad basándose en el **consenso**, que es donde entra en juego el blockchain. Esta **cadena de bloques** es una *base de datos compartida que funciona como un libro para el registro de operaciones* de compra-venta o cualquier otro tipo de transacción.

# ¿Qué es blockchain?



- **Blockchain** se podría decir que es un conjunto de apuntes que están en una base de datos compartida en la que se registran mediante códigos las transacciones realizadas.
  - Usa **claves criptográficas** y al estar distribuido por muchos ordenadores nos presenta ventajas en la seguridad frente a manipulaciones y fraudes.
  - Una modificación en una de las copias sería inútil, ya que se debe realizar el cambio en todas las copias porque la base es abierta y pública.
- Tres grandes **cualidades**: irrefutable, irrevocable y distribuida.



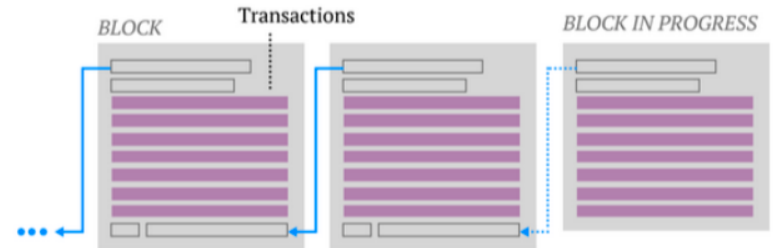
# Componentes

Fundamentos:

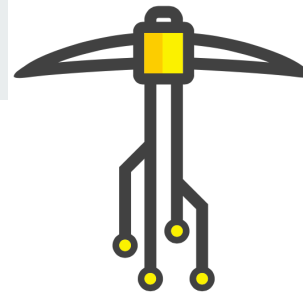
- El registro compartido de las transacciones.
- El consenso para verificar las transacciones.
- Un contrato que determina las reglas de las transacciones.
- La criptografía.

# Bloques

- Blockchain se basa en crear un **registro de todas las transacciones**, y estas se empaquetan en **bloques** que los mineros crean y luego se encargan de verificar. Una vez terminada su validación serán agregadas a la cadena y distribuidas a todos los nodos que forman la red.
- Un **bloque** es un conjunto de **transacciones confirmadas e información adicional** que se ha incluido en la cadena de bloques. Formado por:
  - 1. Un código alfanumérico que enlaza con el bloque anterior.
  - 2. El “paquete” de transacciones que incluye.
  - 3. Otro código alfanumérico que enlazará con el siguiente bloque.



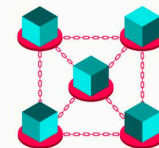
# Mineros



- *Ordenadores dedicados* que aportan su poder computacional a la red para **verificar las transacciones** que se llevan a cabo. Siguen los siguientes pasos:

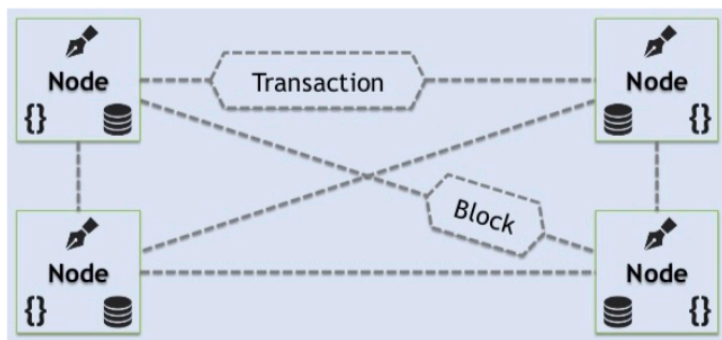
- Las nuevas transacciones se transmiten a todos los nodos.
- Cada nodo de la minería recoge nuevas transacciones en un bloque.
- Cada nodo minero trabaja en la búsqueda de una **prueba de trabajo** para su bloque.
- Cuando un nodo de la minería encuentra y completa dicha prueba de trabajo, este transmite el bloque a todos los nodos.
- Los demás nodos acepta el bloque sólo si todas las transacciones son válidas y no se hayan gastado.
- Los nodos expresan su aceptación del bloque trabajando en la creación del próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash anterior.





# Nodos

- Computadoras conectadas a la red utilizando un software que **almacena y distribuye** una copia actualizada en tiempo real del blockchain.
- Cada vez que un bloque se valida y se añade a la cadena, el cambio es comunicado a todos los nodos y este se añade a la copia que cada uno almacena.





# Características y funcionamiento

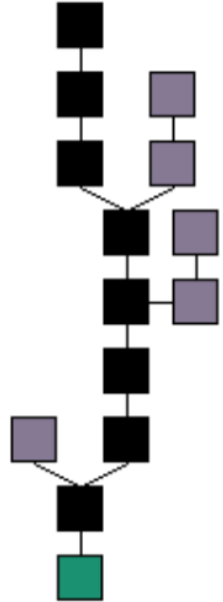
# Descentralizado



- Las redes blockchain son altamente **escalables, descentralizadas y peer-to-peer**.
  - La integridad está basada en un mecanismo de consenso.
  - La red P2P evita que un único participante o grupo controlen el sistema completo.
  - Las transacciones son irreversibles, por lo que una vez realizadas no pueden anularse, modificarse o revertirse.
- Elimina los riesgos que vienen con los sistemas centralizados.
  - La red carece de puntos críticos o centrales de vulnerabilidad que podrían ser explotados.
  - **Criptografía de clave pública:** Una clave pública es una dirección en la cadena de bloque. Los tokens, como por ejemplo bitcoins, son enviados a través de la red y se registran como pertenecientes a esa dirección. Una clave privada es como una contraseña que le da acceso a su propietario a sus activos digitales.

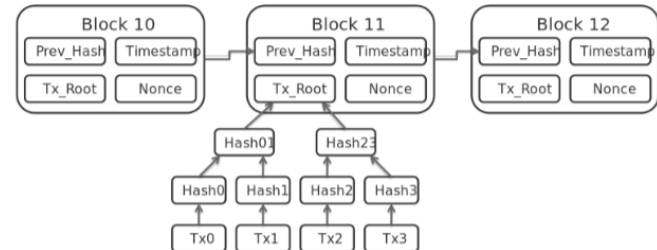
# Sistema abierto

- Cualquier persona puede formar parte tan solo con descargándose el programa. Luego ella podrá realizar movimientos y transacciones y acceder a los datos registrados en su cadena de bloques.
- A veces los bloques se pueden producir concurrentemente, creando un **fork** temporal. Blockchain tiene un algoritmo especificado para marcar diferentes versiones de la cadena para que una con un valor más alto pueda ser seleccionada sobre otras.
- Los peers de la red pueden tener de vez en cuando versiones diferentes de la base de datos.



# Seguridad

- Los bloques que forman parte del blockchain son ordenados en la cadena por orden cronológico y tienen un código alfanumérico conocido como **hash**, que corresponde al bloque que los precede, gracias a ese hash todos están referenciados por el bloque que los creó, por lo que solo los bloques que contienen un código válido son introducidos en la cadena y replicados a todos los nodos.
- Por lo tanto el blockchain nos permite llevar a cabo, una **contabilidad pública de los movimientos** realizados en la red de manera transparente, minimizando la posibilidad de fraude, no permitiendo la pérdida de datos y con un sistema totalmente trazable.





# Aplicaciones

# Aplicaciones



- **Monedas digitales:**

- Descentralizadas, nadie pueda controlarlas, es decir, está fuera del alcance de gobiernos o bancos centrales. Esta independencia de un organismo central es la principal característica respecto al resto de monedas convencionales.

- **Almacenamiento en la nube distribuido:**

- Blockchain permite la creación de un **mercado de almacenamiento distribuido y descentralizado**. Algunos hosts de la red pueden vender su capacidad de storage sobrante y los que necesitan pueden pagar y subir sus archivos los cuales son encriptados, fragmentados y distribuidos inteligentemente por toda la cadena de bloques.

- **Patentes / Registro de propiedad:** Ya que en cada bloque se puede introducir todo tipo de información, incluyendo fechas o timestamps.

# Aplicaciones



## - Smart Contracts:

- Nos ayudan a intercambiar dinero, propiedades, activos o cualquier bien de valor de una manera sencilla, **evitando los gastos por el servicio de intermediarios** y sin revelar ningún tipo de información confidencial sobre las partes y/o naturaleza de la transacción. En este formato *los contratos pueden ser convertidos a código, guardados y replicados en el sistema y supervisados por la red de computadoras que corre el programa blockchain*.

- **Ejemplo:** venta de un automóvil. El comprador obtiene el recibo que es un smart contract, y la llave digital que llega a este en la fecha especificada. Si la llave no llega a tiempo, se le reembolsa el dinero. Si llega, ambas partes reciben lo acordado a tiempo.

- **Premisa de Si-entonces:** Si te doy la llave, de seguro obtengo mi pago, si envías cierta cantidad de bitcoin por ejemplo, recibirás la llave del automóvil.

- **Otras:** Internet of Things, voto electrónico, gobierno transparente, e-commerce e identificación.

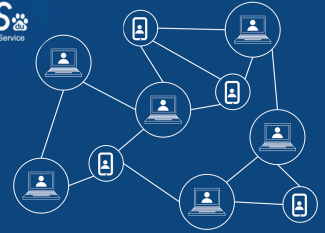




# **Blockchain as a Service**

# Blockchain as a Service

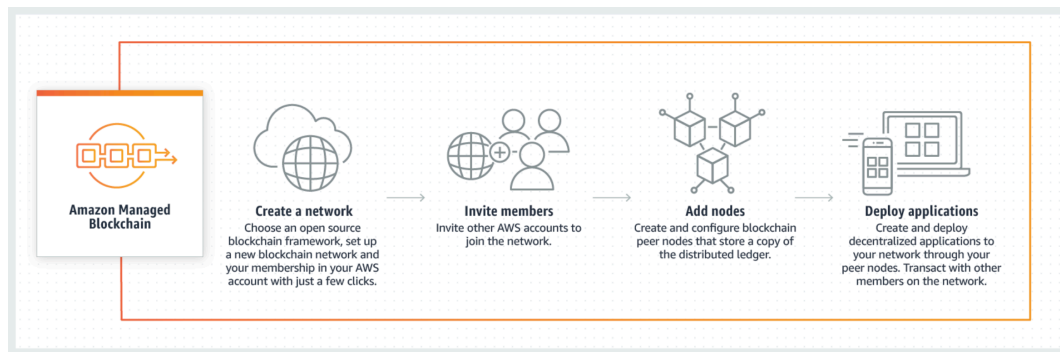
BaaS  
Blockchain as a Service



- BaaS significa que un *proveedor de servicios externo proporciona toda la “tecnología e infraestructura de blockchain”* necesaria para un cliente a cambio de un precio. Al pagar por el BaaS, el cliente paga al proveedor del BaaS para que este configure y mantenga los nodos conectados en el blockchain en su nombre. Además, maneja el complejo back-end para el cliente y su negocio.
- El **operador** BaaS es responsable del buen funcionamiento de los componentes de software y la infraestructura asociados. También realiza funciones adicionales, como la gestión del ancho de banda, la asignación óptima de recursos, el cumplimiento de los requisitos de alojamiento así como funciones de seguridad, como la prevención de ataques de piratas informáticos.
- Al usar el modelo BaaS, en lugar de preocuparse por la infraestructura, *el cliente puede concentrarse en su tarea principal*, que no es otra que el funcionamiento de su propio blockchain y aumentar la productividad.
- En definitiva la idea que sigue BaaS es que **el proveedor nos proporciona toda la infraestructura y nosotros solo tenemos que lanzar nuestra aplicación**. Aunque como veremos, esto aún está empezando a desempeñarse.

# Amazon

- **Amazon Managed Blockchain:** Servicio completamente administrado que facilita la creación y administración de redes de blockchain escalables mediante el uso de los marcos de código abierto populares Hyperledger Fabric y Ethereum\*.



- **Amazon Quantum Ledger Database:** Base de datos de contabilidad completamente administrada en la que se proporciona un registro de transacciones transparente, inmutable y que se puede verificar mediante criptografía, cuya propiedad denota una autoridad central de confianza.

# Azure

- **Azure Blockchain Workbench:** Esta herramienta permite a los desarrolladores desplegar un libro mayor de cadenas de bloques junto con un conjunto de servicios relevantes de Azure que se utilizan con más frecuencia para construir una aplicación basada en cadenas de bloques.


Ponga en marcha rápidamente su proyecto de cadena de bloques en Azure

Soluciones de Marketplace

Asociados


Cree soluciones con el libro de contabilidad que se ajusta a su caso de uso

[Ir a Azure Marketplace >](#)




**Corda**

Utilice la plataforma de libro de contabilidad distribuida Corda para implementar una red multinodo de varios participantes, además de un mapa de red, notarias e iguales.



**Ethereum**

Implemente una gran variedad de tecnologías de red de Ethereum en cuestión de minutos. Administre nodos con implementaciones entre varias regiones, VM Scale Sets y supervisión.



**Hyperledger Fabric**

Ponga en marcha una red Hyperledger Fabric en solo unos minutos e implemente servicios para miembros, la realización de pedidos y la validación de iguales.



# GRACIAS

¿Preguntas?

Más información: <https://github.com/luiisgallego/Blockchain>

Luis Gallego Quero