



Blockchain

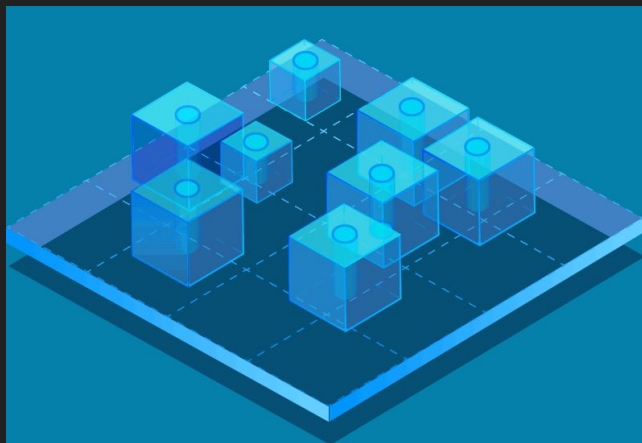
Kevin Lajpop
Java Day 2018

Acerca de ...

- Ingeniero en Ciencias y Sistemas
- Candidato a Máster en TICs
- Coordinador de desarrollo -SENACYT-
- Amante de la ciencia y el arte
- Guitarrista y bajista de afición
- Eterno estudiante de la vida



Contenido



- Calentando motores ¿Block... qué?
- Blockchain
- Tipos de blockchain
- Principios de blockchain
- Componentes de blockchain
- Roles y participantes
- Ventajas
- Aplicaciones
- ¿El futuro?

Calentando Motores ¿Block... qué?

- ¿Se han imaginado un lugar donde las personas sean verdaderas dueñas de su información?
- ¿Se han imaginado un lugar donde no se pueda alterar un dato para un fin perverso?
- ¿Se han imaginado un lugar donde no exista riesgo de pérdida de información?

Blockchain

Blockchain funciona como un libro mayor de transacciones, dichas transacciones se agrupan en bloques y los bloques forman la cadena.

Blockchain

Es una estructura de datos la cual tiene forma de una lista enlazada que utiliza punteros hash en lugar punteros normales como se utilizarían en listas normales, los punteros hash sirven para enlazar al bloque anterior.

Tipos de Blockchain

Blockchain Público

Un blockchain público es aquel que no tiene ninguna restricción para leer los datos del blockchain y de igual manera es fácil entrar y salir del blockchain, siendo las transacciones transparentes. Un ejemplo de ellas son las criptomonedas como Bitcoin o Ethereum.

Blockchain Privado

Un blockchain privado es aquel que solo los que se designan como propietarios (una lista de entidades predefinida) tienen acceso a los datos o a la cadena y de igual manera el ingreso de transacciones a la misma.



Principios de Blockchain

Integridad

La integridad está a lo largo de la cadena y nodos que forman parte del blockchain, por lo que, lo que quiere decir que no depende de un componente aislado la integridad de la información.

Poder distribuido

El poder está distribuido a todos los nodos de la cadena, no existe un poder centralizador, blockchain es público para todos los nodos, por lo que si existe algún movimiento extraño dentro de la cadena todos lo verían dejando el poder de decisión a todos los nodos miembros de la cadena.

Principios de Blockchain

Seguridad

La seguridad de un blockchain está centrada en el uso de criptografía, es decir, todos los nodos miembros deben de utilizar criptografía para formar parte de un blockchain, caso contrario no podrán formar parte de uno.

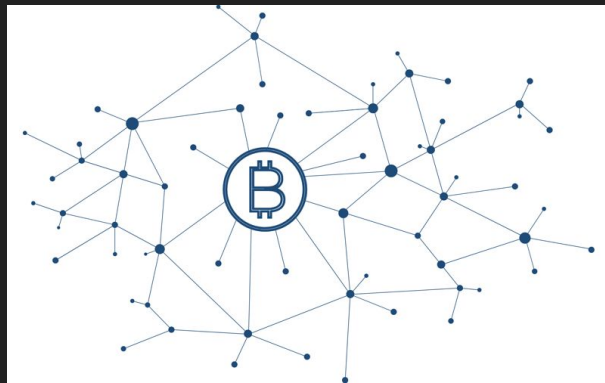
Privacidad

Los datos de una persona o entidad dentro de un blockchain son únicamente de las personas, no más, no menos, respetando la privacidad de los mismos.

Principios de Blockchain

Derechos Preservados

Los miembros de un blockchain tienen derechos y estos derechos se respetan, tal es el caso del derecho a privacidad, es decir que en mundo digital del blockchain se respetan los derechos.



Componentes de Blockchain

Bloques

Toda la información que entra a un blockchain es almacenada en un bloque, y este bloque añadido a la cadena. El bloque es la unidad básica de almacenamiento del blockchain.

Componentes de Blockchain

Bloques

Cada bloque debe de tener como mínimo la siguiente información:

- Código que enlaza con el bloque anterior.
- La información como tal que se almacena.
- Código que enlaza con el bloque siguiente.

Componentes de Blockchain

Mineros

Un minero es una máquina que ayuda en el proceso de validación de transacciones que se producen, autorizando la agregación de nuevos bloques

Componentes de Blockchain

Mineros - Acciones

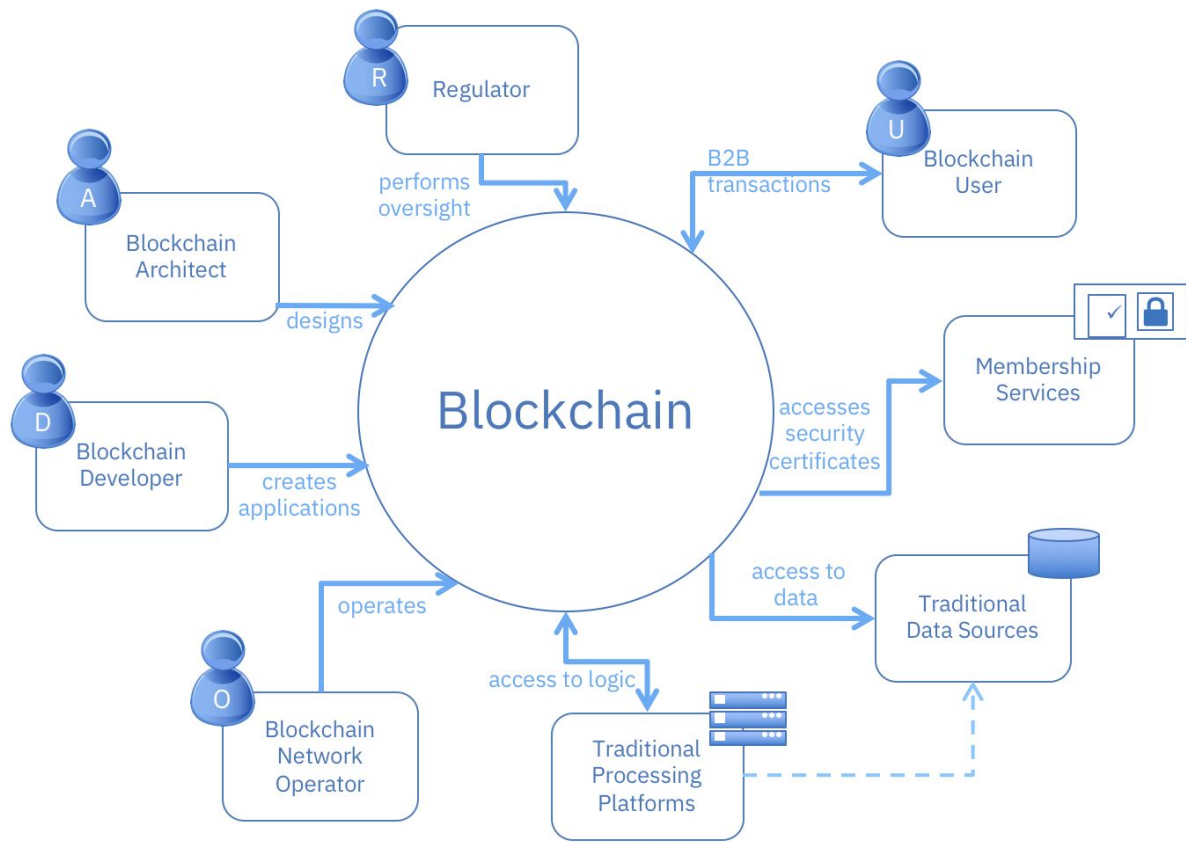
- Reciben las nuevas transacciones.
- Recogen la nueva transacción y la almacenan en un bloque.
- Buscan una prueba de trabajo para el bloque.
- Transfiere el bloque a todos los nodos.
- Aceptan la transacción solo si las transacciones son válidas.
- Los nodos aceptan el bloque creando el bloque siguiente colocando el hash anterior en el nuevo hash.

Componentes de Blockchain

Nodos

El nodo es una máquina conectada a una red, cuenta con un software que permite el almacenamiento y la distribución de una copia real del blockchain.

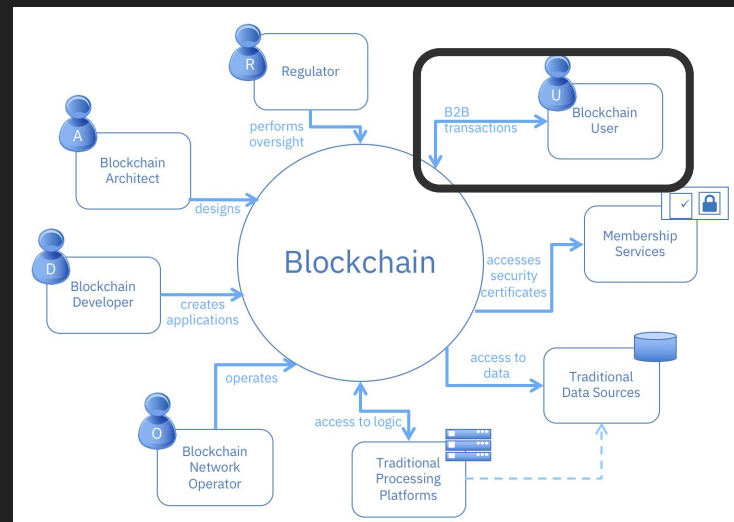
Roles y participantes



Roles y participantes

Usuario de la cadena

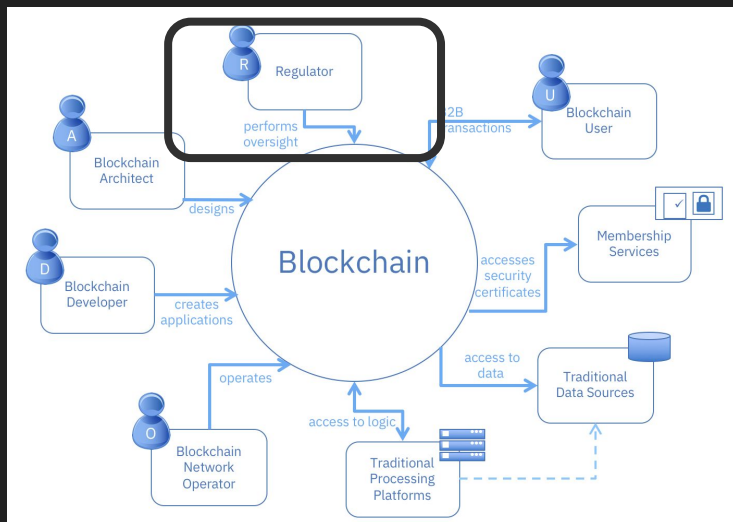
Un participante con permisos para unirse a la red de blockchain y realizar transacciones con otros participantes de la misma red.



Roles y participantes

Regulador

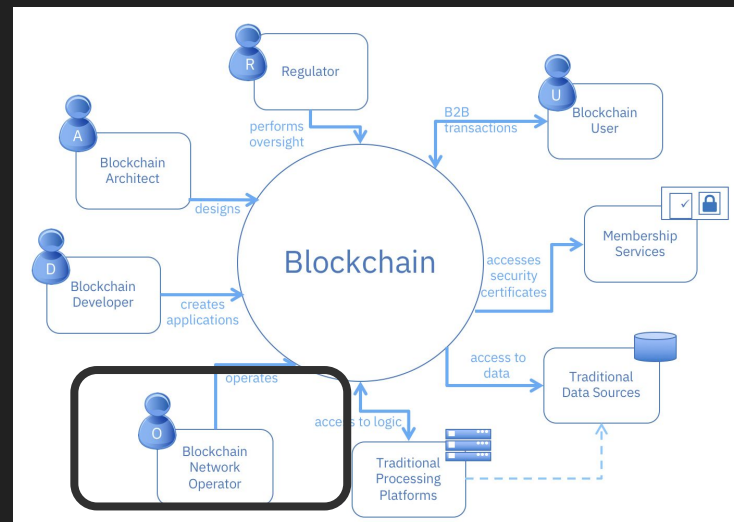
Un usuario de blockchain con permisos especiales para supervisar las transacciones que ocurren dentro de la red. Hay que tener en cuenta que los reguladores pueden tener prohibido realizar transacciones.



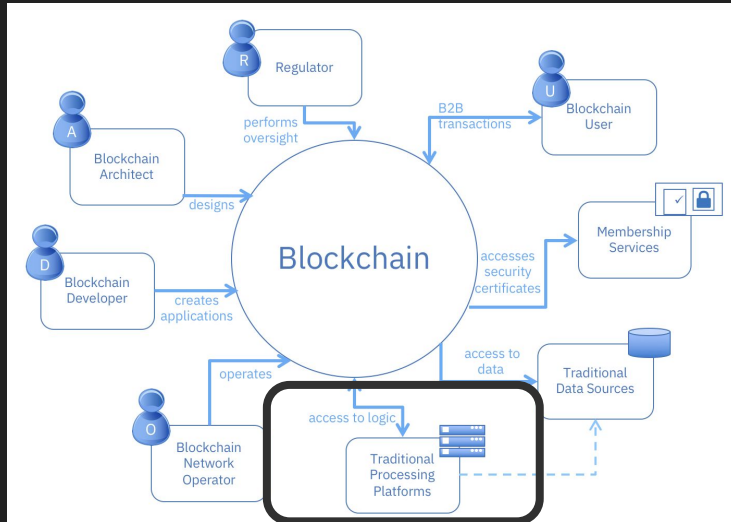
Roles y participantes

Operador de red de blockchain

Personas que tienen permisos especiales y autoridad para definir, crear, administrar y monitorear la red de blockchain. Cada entidad que forma parte de la red de blockchain debe de tener un operador de red de blockchain.



Roles y participantes



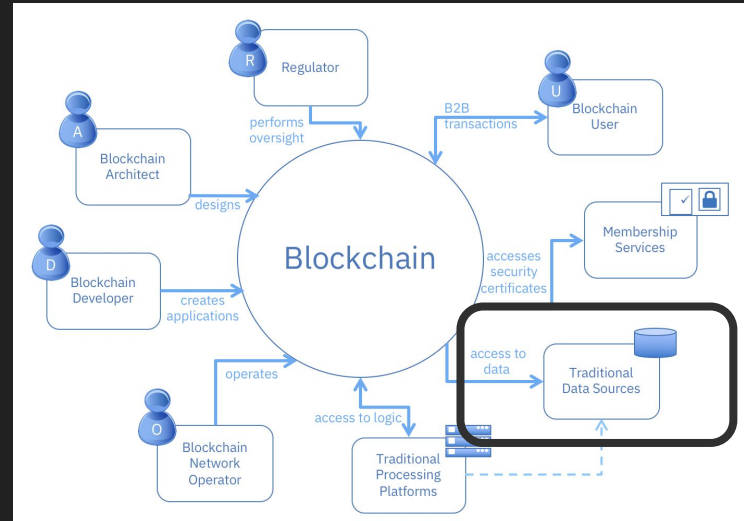
Plataformas de procesamiento tradicionales

Sistemas de información existentes que pueden ser utilizados por el blockchain para aumentar el poder de procesamiento. Este sistema también puede interactuar vía solicitudes en el blockchain.

Roles y participantes

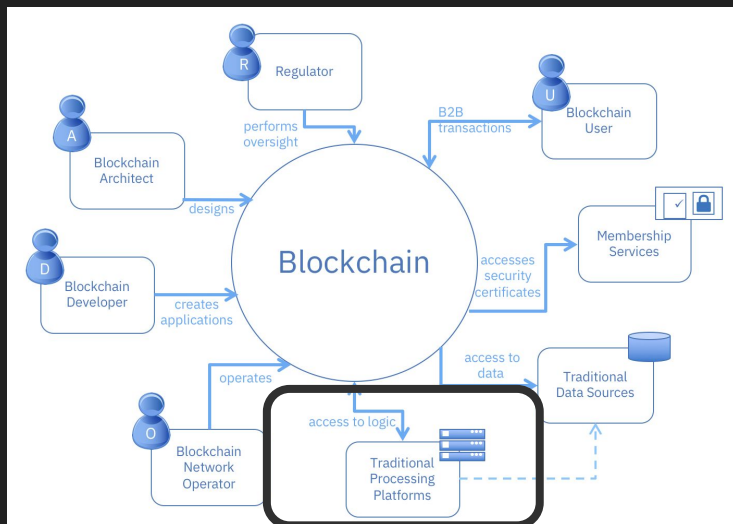
Fuentes de datos tradicionales

Los sistemas de datos existentes pueden proporcionar datos para influir en el comportamiento de los contratos inteligentes y ayudar a definir cómo se producirán las comunicaciones y la transferencia de datos entre las aplicaciones y datos tradicionales con el blockchain.



Roles y participantes

Autoridad de certificación

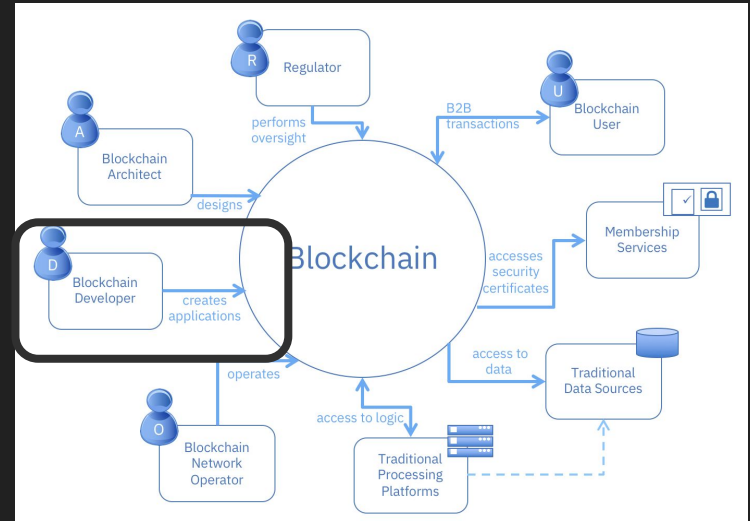


Una persona o entidad que emite y administra los diferentes tipos de certificados requeridos para ejecutar un blockchain con sus diferentes permisos.

Roles y participantes

Desarrollador Blockchain

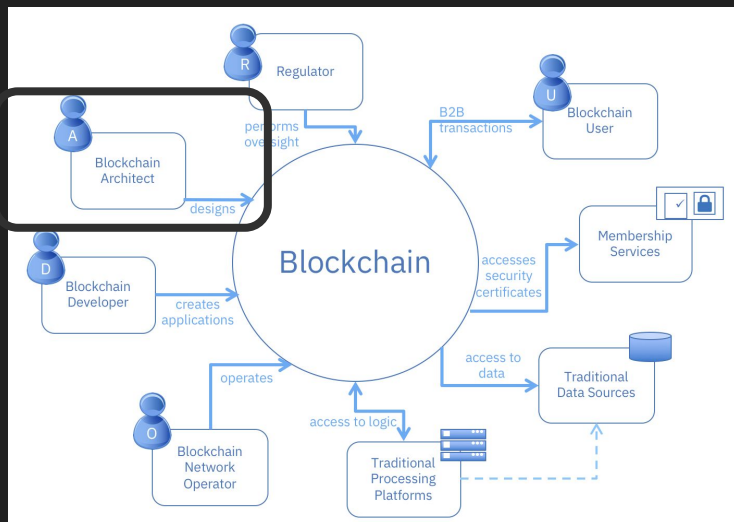
Programadores que realizan aplicaciones y los contratos inteligentes que permiten a los usuarios de blockchain realizar transacciones.



Roles y participantes

Arquitecto Blockchain

Persona encargada de todo el diseño de la cadena.



Ventajas de blockchain

Ventajas de blockchain

Libro contable

Blockchain trabaja en base a los principios de un libro de contabilidad, solamente que es distribuido y compartido, es decir, un registro inmutable del libro está en toda la red y todos los participantes de la red pueden acceder.

[illegible]

Ventajas de blockchain



Permisos

En una cadena de bloques, cada participante tiene una identidad única, que permite el uso de políticas para restringir la participación en la red y el acceso a las transacciones. Con la capacidad de restringir el acceso a la red también son más efectivas para controlar la consistencia de los datos que se adjuntan a la cadena de bloques.

Ventajas de blockchain

Consenso

En una red de bloques donde los participantes son conocidos y confiables, las transacciones pueden verificarse y comprometerse con el libro de contabilidad a través de varios medios de acuerdos (consenso).



Ventajas de blockchain



Contratos inteligentes

Un contrato inteligente es un acuerdo o conjunto de reglas que rigen una transacción; un contrato inteligente se almacena en la cadena de bloques y se ejecuta automáticamente como parte de una transacción.

Aplicaciones

Aplicaciones

- **Criptomonedas**
- **Almacenamiento en la nube distribuido**
- **Internet de las cosas**
- **Identificación**
- **Contratos Inteligentes**
- **Patentes / Registro de la propiedad**
- **Voto electrónico**
- **Transparencia**

Dudas, comentarios

