ESTUDIO DEL MERCADO DE CRIPTOACTIVOS EN EL ECUADOR

Comité de Innovación Financiera
Mesa Cripto

Clúster Financiero

Estudio del mercado de criptoactivos en el Ecuador

INTRODUCCIÓN

Conceptos Básicos

Blockchain:

Es una tecnología con infraestructura distribuida, es como un libro de contabilidad, o una notaría, descentralizada, donde a través de funciones matemáticas, que realizan, los nodos (Equipos de cómputo), guardan el registro de las transacciones realizadas, es encriptado e inmutable y permite el intercambio de datos de manera descentralizada.

Criptoactivos:

Un criptoactivo es un tipo de activo virtual, el cual tiene su origen en la criptografía. Los diferentes criptoactivos poseen un determinado valor de mercado, el cual nos permite, en caso de poseerlos, generar ingresos al venderlos o al intercambiarlos por bienes o servicios.

Existen dos grandes grupos de criptoactivos: tokens y criptomonedas.

Token:

En términos simples, un token es la representación digital en el mundo Blockchain, un token puede ser físico o virtual, incluso puede representar un concepto abstracto.

Cualquier activo (físico o virtual) puede ser “Tokenizado” y colocado en una red blockchain, una vez allí, puede ser transado en diferentes mercados, se puede comprar y vender, hipotecar, ser ofrecido en título valor, alquilar o fraccionar.

Token no fungible, Non Fungible Token o NFT:

Son activos únicos, un NFT es el título de propiedad de un activo único dentro de una blockchain.

Al momento su mayor aplicabilidad se ha dado en el mundo del arte, sin embargo, puede aplicarse a la compra de activos físicos, bienes raíces, productos exclusivos y más.

DApp (Decentralized Application):

Su definición es Aplicaciones Descentralizadas, es una aplicación que no depende de servidores centralizados (AWS por ejem.) ya que su funcionamiento se realiza sobre una red descentralizada (Blockchain). Las DApps no tuvieron mayor relevancia hasta la llegada de Ethereum y Solidity (Lenguaje de programación).

En las DApps, el backend (capa de programación de una aplicación), está asociado a un contrato inteligente que se ejecuta sobre una blockchain (Cadena de bloques). Los contratos inteligentes son 100% públicos y visibles, garantizando un alto nivel de transparencia y seguridad para los usuarios.

Wallet:

Se las usa para enviar y recibir criptoactivos, se pueden encontrar software wallets, hardware wallets y paper wallets

Exchange:

Son los mercados para criptoactivos, donde se pueden comprar y vender los mismo

DAO

Es una Organización Autónoma Descentralizada (DAO por sus siglas en inglés). Una DAO es una comunidad que trabaja en conjunto para cumplir una misión; las decisiones son tomadas únicamente por los miembros de la comunidad y cada uno de ellos tiene la capacidad de votar.

Dentro de toda organización es importante conocer quién toma las decisiones y cómo lo hace. Las Organizaciones Autónomas Descentralizadas están basadas en blockchain y las reglas del juego definidas dentro de smart contracts, que son scripts de código que realizan una acción determinada a partir de un evento.

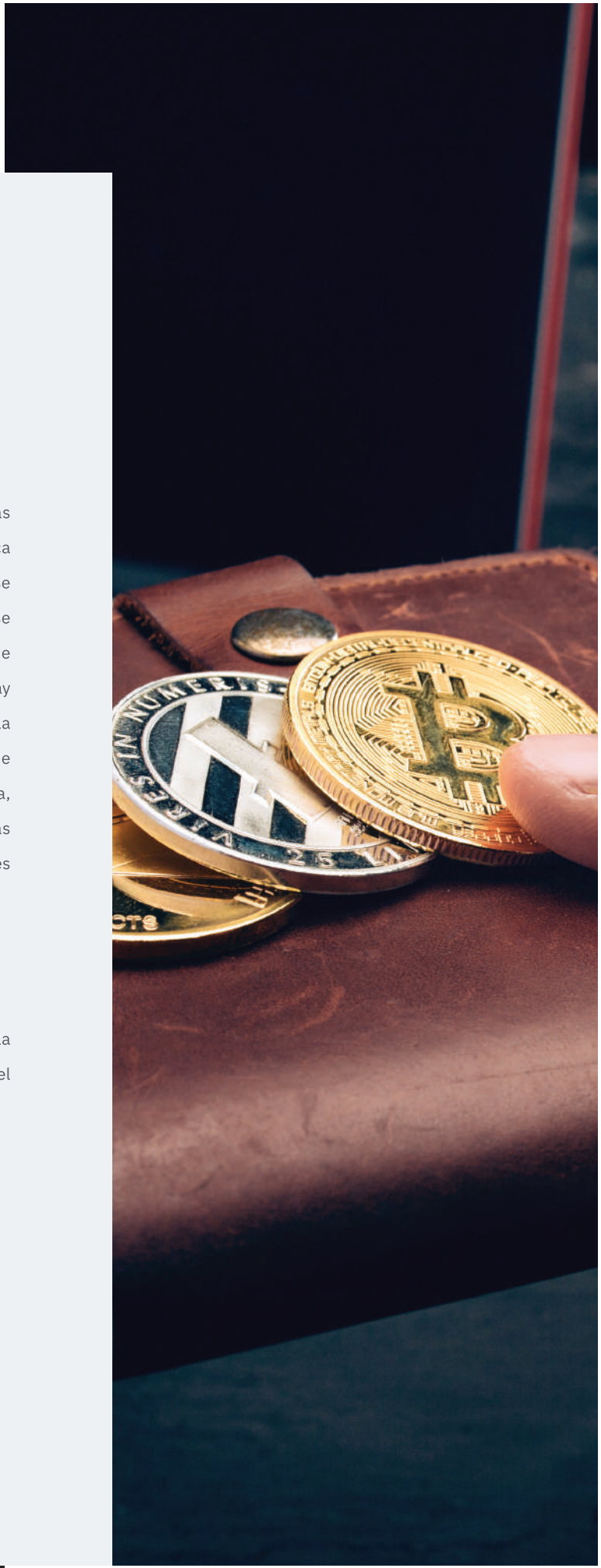
Finanzas descentralizadas, Decentralized finance o DeFi.

DeFi, abreviatura de "finanzas descentralizadas", es un término que engloba un grupo de herramientas financieras construidas sobre una blockchain.

La idea es permitir que cualquier persona con acceso a Internet pueda prestar, pedir prestado y realizar operaciones bancarias sin pasar por intermediarios.

La emisión y la existencia de las monedas digitales se dan en una base de datos pública que es mantenida por lo que generalmente se conoce como blockchain. La base de datos se distribuye en todas las computadoras que ejecutan el software de la blockchain. No hay una entidad en particular que sea dueña de la base de datos o la controle, sino que cualquier usuario puede acceder a ella, exhibir titularidad o realizar transferencias con criptomonedas mediante las claves privadas asociadas a su billetera cripto.

FUENTE: NFTs: Cómo promover la participación de los fanáticos de hoy en el entorno cripto y de comercio. VISA



INFRAESTRUCTURA:
LA TECNOLOGÍA BLOCKCHAIN

Definición

4. Nociones Fundamentales del Blockchain

Blockchain o en español “Cadena de bloques” es – esencialmente- una base de datos descentralizada que combina tecnologías ya existentes para crear redes que aseguran la confianza entre personas y partes que de otro modo no tuvieran razón de confiar entre sí1. Ella es una es una brillante amalgama de conceptos de criptografía, teoría de juegos e ingeniería de ciencia computacional2.

Blockchain emplea un método de cifrado conocido como criptografía y utiliza (un conjunto de) algoritmos matemáticos específicos para crear y verificar una estructura de datos en continuo crecimiento, a la que solo se pueden agregar datos y de la cual no se pueden eliminar los datos existentes, que toma la forma de una cadena de "bloques de transacciones" [De ahí el nombre cadena de bloques], que funciona como un libro mayor distribuido. En la práctica, blockchain es una tecnología con muchas “caras” pues puede exhibir diferentes características y cubre una amplia gama de sistemas que van desde ser completamente abiertos y no permisionados, hasta permisionados3. De estos tipos de Blockchain se tratará más adelante

Las tecnologías que se combinan para formar blockchain son:

- LT (Descentralized Ledger Technologies o Tecnologías de libro mayor distribuido) para almacenar la información. La expresión “libro mayor distribuido” se refiere a una base de datos que mantienen información a través de una red de servidores de manera descentralizada o distribuida4. Cada servidor es un “nodo” que contiene exactamente los mismos registros de datos que el resto.
- Criptografía para verificar la información, asegurar su integridad y confidencialidad, y autenticar quién es el emisor que envía la información5.
- Protocolo de consenso para garantizar la congruencia de los datos6.

Blockchain, a menudo, se utilizan para emitir y transferir la propiedad de activos digitales

¿CÓMO FUNCIONA LA TECNOLOGÍA BLOCKCHAIN?

A fin de explicar el funcionamiento de la cadena de bloques, estableceremos algunos puntos clave a partir de los cuales se desarrollará una explicación básica de su funcionamiento:

a.

Blockchain es una base de datos distribuida

Como se refirió, Blockchain es – en términos simples- una base de datos distribuida. Las adiciones o registro a esta base de datos son

iniciadas por uno de los miembros (es decir, los nodos de la red), que crea un nuevo "bloque" de datos, que puede contener todo tipo de información. Luego, este nuevo bloque se transmite a todas las partes de la red de forma encriptada (utilizando criptografía). Los otros nodos de la red determinan colectivamente la validez del bloque de acuerdo con un método de validación algorítmico predefinido, comúnmente denominado "mecanismo de consenso". Una vez validado, el nuevo "bloque" se agrega a la cadena de bloques, lo que esencialmente resulta en una actualización del libro mayor de transacciones que se distribuye a través de la red7.

b.

Las transacciones contenidas en los bloques son firmadas digitalmente empleando una llave privada8

Cada usuario en una red blockchain tiene un conjunto de dos claves. Una clave privada, que se utiliza para crear una firma digital para una transacción, y una clave pública, que todos conocen en la red. La clave pública tiene dos usos: 1) sirve como dirección en la red blockchain; y 2) se utiliza para verificar una firma digital / validar la identidad del remitente.

Las claves públicas y privadas de un usuario se guardan en una billetera digital o billetera electrónica (en inglés wallet). Dicha billetera puede almacenarse o guardarse en línea (el almacenamiento en línea a menudo se denomina "almacenamiento activo") y/o fuera de línea (el almacenamiento fuera de línea se denomina comúnmente "almacenamiento en frío"). De ahí las referencia a hot wallet y cold wallet.

c.

Los mecanismos o protocolos de consenso9

En principio, cualquier nodo dentro de una red blockchain puede proponer la adición de nueva información a la cadena de bloques. Para validar si esta adición de información (por ejemplo, un registro de transacción) es legítima, los nodos deben llegar a algún tipo de acuerdo. Aquí es donde entra en juego el llamado “mecanismo de consenso” o “protocolo de consenso”. En resumen, un mecanismo de consenso es un método de validación específico (criptográfico) predefinido que garantiza una secuencia correcta de transacciones en la cadena de bloques. En el caso de las criptomonedas, se requiere tal secuencia para abordar el problema del "doble gasto" (es decir, el problema de que un mismo instrumento de pago o activo puede transferirse más de una vez si las transferencias no se registran y controlan de forma centralizada).

Un mecanismo de consenso se puede estructurar de varias maneras. Los dos ejemplos de mecanismos de consenso más conocidos y más utilizados son el mecanismo de prueba de trabajo ("PoW, del inglés “Proof of Work”) y el mecanismo de prueba de participación ("PoS", del inglés “Proof of Stake”). Más adelante se explicará el funcionamiento de cada uno.

CARACTERÍSTICAS CLAVE

Lo descrito hasta ahora respecto de la cadena de bloques se traduce a su vez en una serie de características clave que nos servirán como base para después analizar el potencial que tiene esta tecnología. En ese orden de ideas, blockchain es:

- Distribuido: la base de datos es mantenida y conservada por todos los nodos de la red. Ninguna autoridad central mantiene o actualiza la base de datos, sino que cada nodo de manera independiente construye su propio registro procesando cada bloque (grupo de transacciones), decidiendo si es válido y luego votando sobre sus conclusiones por medio de un mecanismo de consenso. Una vez que un cambio en el registro es acordado, cada nodo actualiza su base de datos.

- Inmutable: en general, una vez una transacción es añadida a la cadena de bloques, no puede deshacerse. Esta inmutabilidad es uno de los principales aspectos que contribuyen a la fiabilidad que se tiene sobre las transacciones de la Blockchain. La inmutabilidad de la cadena de bloques es asegurada por medio de su uso de criptografía.

- Acordado por consenso: ningún bloque puede ser añadido a la base de datos sin la aprobación de nodos específicos en la red. Las reglas respecto de cómo este consentimiento se recolecta son llamadas “mecanismos o protocolos de consenso”. Los protocolos de consenso son cruciales para asegurar que cada bloque es válido y que todos los participantes acuerdan y mantienen la misma versión del registro. Ellos afectan gravemente los incentivos de los nodos para actuar honestamente y son, por tanto, las variables más importantes cuando se diseña una Blockchain.

- Seudonimidad: en general la cadena de bloques no permite que sus usuarios sean completamente anónim

n realidad, las Blockchain públicas tienden a usar seudónimos: las identidades de los usuarios pueden ser anónimas pero las direcciones no pues todas sus transacciones son visibles para todos los usuarios. En estas plataformas las cuentas pueden crearse sin ningún proceso de identificación o autorización. Esto permite a los usuarios emplear un pseudónimo. La consecuencia de esto es que con suficiente información es posible rastrear la actividad a direcciones particulares y direcciones a individuos o partes (personas) involucradas en la cadena de bloques. No obstante, es preciso destacar que existen ciertas criptomonedas que han sido especialmente diseñadas para resolver este tema de seudonimidad y enmascaran la identidad de los participantes (ejemplos son: Z-Cash y Monero)10.

En el caso de las Blockchain permisionadas, ellas pueden requerir que la identidad del usuario se verifique antes de que pueda acceder o usar la cadena de bloques. Más adelante se explica la distinción entre los diferentes tipos de Blockchain.

ETHEREUM: DEL SIMPLE «REGISTRO» A LAS APLICACIONES DESCENTRALIZADAS (DAPPs)

En 2015 se lanzó Ethereum. Una plataforma descentralizada (más técnicamente una blockchain pública no permisionada) que trajo una importante revolución: ahora cualquiera podía crear aplicaciones sobre Blockchain para realizar diversas tareas. Se trata de un sistema operativo como los que se encuentran en los teléfonos inteligentes; cualquiera puede crear aplicaciones sobre la plataforma para realizar diversas tareas. Esto distinguió a Ethereum de Bitcoin. Bitcoin fue diseñado específicamente para limitarse a la lógica simple, como un sistema de efectivo electrónico entre pares (peer-to-peer). Ethereum admite código de programación para cualquier tipo de aplicación descentralizada; su capacidad es más amplia. La plataforma ejecuta contratos inteligentes11.

Los contratos inteligentes son contratos o aplicaciones de "ejecución automática" que se ejecutan exactamente según lo programado sin ninguna posibilidad de tiempo de inactividad (es decir, blockchain nunca se cae, siempre se está ejecutando), censura, fraude o interferencia de terceros.

Al igual que otras cadenas de bloques abiertas y no permisionadas, Ethereum requiere una forma de valor On Chain para incentivar la validación de transacciones dentro de la red (es decir, una forma de pago para los nodos de la red que ejecutan las operaciones). Aquí es donde entra en juego la criptomoneda nativa "Ether" (ETH) de Ethereum. Ether no solo permite que se construyan contratos inteligentes en la plataforma Ethereum (es decir, los alimenta), sino que también funciona como un medio de intercambio (específicamente en el contexto de las Inital Token Offering, ya que muchos tokens se compran con ether)12.

Al igual que Bitcoin, Ethereum actualmente utiliza un mecanismo de consenso PoW, pero se está moviendo lentamente hacia la adopción de un mecanismo de consenso PoS.

EL POTENCIAL DE BLOCKCHAIN

Lo descrito hasta ahora respecto de la cadena de bloques se traduce a su vez en una serie de características clave que nos servirán como base para después analizar el potencial que tiene esta tecnología. En ese orden de ideas, blockchain es:

BEGINNING BLOCKCHAIN:
A BEGINNER'S GUIDE TO BUILD BLOCKCHAIN SOLUTIONS

Blockchain ha llegado ahora para llevar al Internet a un nivel completamente nuevo removiendo las fricciones en tres áreas clave: control, confianza y valor.

- Control: blockchain permite la distribución del control haciendo descentralizados a los sistemas.
- Confianza: Blockchain es un registro contable inmutable y resistente a la manipulación. Provee una única fuente compartida de verdad para todos los nodos, haciendo de "0 Confianza" (trusless) a su entorno. Lo que esto significa es que la confianza ya no es requerida para transar con ninguna persona o entidad desconocida, sino que la confianza es inherente al diseño y a la misma tecnología.
- Valor: Blockchain permite el intercambio de valor en cualquier forma. Un puede emitir y transferir activos sin la necesidad de una entidad central o intermediarios.

HOUBEN, R. y SNYERS, A. (2018):

¿Eliminando al intermediario?

"Una de las principales ventajas de la tecnología blockchain es que permite simplificar la ejecución de una amplia gama de transacciones que normalmente requerirían la intermediación de un tercero (por ejemplo, un custodio, un banco, un sistema de liquidación de valores, agentes de bolsa, un registro de operaciones, ...). En esencia, blockchain trata de descentralizar la confianza y permitir la autenticación descentralizada de transacciones. En pocas palabras, permite eliminar al "intermediario" [30].

En muchos casos, esto probablemente conducirá a ganancias de eficiencia. Sin embargo, es importante subrayar que también puede exponer a las partes interactuantes a ciertos riesgos que anteriormente eran manejados por estos intermediarios. Por ejemplo, el Banco de Pagos Internacionales ("BIS") advirtió recientemente en un informe de 2017 titulado Tecnología de libro mayor distribuido en pagos, compensación y liquidación, que la adopción de la tecnología blockchain podría introducir nuevos riesgos de liquidez. Más en general, parece que cuando un intermediario funciona como un amortiguador contra riesgos importantes, como el riesgo sistémico, no puede ser reemplazado simplemente por la tecnología blockchain" (pp.17-18)

30 Cabe señalar que en las cadenas de bloques permisionadas todavía hay un papel para una parte central.

Blockchain: casos de uso reales

Si bien blockchain es a menudo asociado con esquemas de activos virtuales o digitales, pagos o servicios financieros, es importante tener presente que su ámbito de aplicación es mucho más amplio tanto respecto de los sectores como de los casos de uso. En el presente apartado dejamos una breve revisión de casos de uso reales.

2. Mecanismos de consenso de blockchain

PRUEBA DE TRABAJO (PoW, del inglés “Proof of Work”)

IFRS (#) Accounting for crypto-assets (EY) (2018)

“La prueba de trabajo es el protocolo de consenso de blockchain original, iniciado por Bitcoin. En un sistema de prueba de trabajo, los participantes de la red compiten para ser los más rápidos en resolver los acertijos criptográficos necesarios para agregar un nuevo bloque a la cadena de bloques. La entrada [input] a estos acertijos consiste en toda la información previamente registrada en la cadena de bloques, junto con el nuevo conjunto de transacciones que se agregará en el siguiente bloque. Por lo tanto, la entrada [input] se vuelve más grande y el cálculo más complejo con el tiempo, lo que requiere una mayor potencia de procesamiento. [...]

Cuando se resuelve el rompecabezas, la máquina involucrada demuestra que completó el trabajo y es recompensada en cualquier sistema dado con una ficha de valor. En la cadena de bloques de Bitcoin, esto se presenta en forma de un bitcoin recién extraído.

Tenga en cuenta que si bien la minería exitosa se recompensa con nuevos bitcoins, uno no tiene que poseer ningún bitcoin como requisito previo para participar en la minería de bitcoins.” (p.17)

PRUEBA DE PARTICIPACIÓN

(PoS, del inglés “Proof of Stake”)

Una diferencia clave de este protocolo de consenso respecto del PoW es precisamente el requerir una participación. El PoW no requiere que se tenga una participación (por ejemplo, tener un Bitcoin para minar en la red de bitcoin) como prerrequisito para participar en la validación de transacciones. Adicionalmente, a diferencia del PoW, el PoS requiere poco poder de cómputo y electricidad.

3. Los contratos inteligentes

Los contratos en papel son escritos en lenguaje natural. Es decir, basta con redactar las condiciones y términos en el idioma implicado. Si todas las partes están de acuerdo, firman para asegurar su promesa, lo cual nos lleva a su implicación legal: un contrato en papel tiene costes. Según la jurisdicción donde se encuentren los involucrados, o bajo la que quieran llevar a cabo el contrato, es muy probable que tengan que cumplir con ciertos requisitos, como recurrir a una notaría. Por otro lado, su modo de cumplimiento está sujeto a la interpretación de las partes, que puede llegar a favorecer a una más que a la otra.

Los contratos inteligentes, en cambio, son programas informáticos. No están escritos en lenguaje natural, sino en código virtual. Son un tipo de software que se programa, como cualquier otro software, para llevar a cabo una tarea o serie de tareas determinadas de acuerdo a las instrucciones previamente introducidas. Su cumplimiento, por tanto, no está sujeto a la interpretación de ninguna de las partes: si el evento A sucede, entonces la consecuencia B se pondrá en marcha de forma automática. Su implicación legal ha caído —como toda la tecnología relacionada a Bitcoin— en una zona gris. No se requiere de ningún intermediario de confianza (como una notaría), pues este papel lo adopta el código informático, que asegurará sin dudas el cumplimiento de las condiciones. Por tanto, se reducen tiempo y costes significativos.}

Un ejemplo de uso puede ser una apuesta deportiva. Digamos que María quiere apostar X bitcoin al equipo A, y Pedro quiere apostar la misma cantidad al equipo B. Depositan los fondos en un contrato inteligente para asegurarse de que, tras el resultado, el ganador realmente se quede con ellos. Pero, ¿quién le dice al contrato cuál de los equipos ganó? La respuesta es el oráculo (oracle). Estas son herramientas informáticas que permiten actualizar el estado de los contratos inteligentes con información del exterior, como los precios de las divisas, la cotización de las acciones o si ganó el equipo A o el B. Aunque, por supuesto, la fuente de ese oráculo sigue siendo una tercera parte, un intermediario fuera de la blockchain y fuera del contrato y por tanto sujeto a la confianza. Este es un problema a resolver, pues precisamente lo que se quiere eliminar con los smarts contracts y la blockchain es la necesidad de confianza.

4. Tipos de Blockchain

Si bien hay un gran número de características variables, dos de las más importantes son la apertura de la plataforma (público o privado) y el nivel de permiso requerido para añadir información a la Blockchain (permisionado o no permisionado)

- Blockchain pública: cualquier persona puede leer y ver las transacciones. Ejemplo: Bitcoin, Ethereum, Ripple, Polygon, Solana, Cardano, entre otras.
- Blockchain privada: la información solo puede ser vista por un grupo escogido de personas, como ejemplo puede ser Quorum de JP Morgan.
- Blockchain permisionada: solamente permiten a un determinado grupo selecto escribir (esto es, generar transacciones para ser grabadas en el registro) y participar (esto es, verificar nuevos bloques para ser adicionados a la cadena).
- Blockchain no permisionada: permite a cualquiera contribuir y añadir datos al registro.

			Leer	Escribir	Participar	Ejemplo
Tipos de Blockchain	Abierta	Pública no permisionada	Abierta a cualquiera	Cualquiera	Cualquiera	Bitcoin, Ethereum
		Públic permisionada	Abierta a cualquiera	Participantes autorizados	Todos o una parte de los participantes autorizados	Registro de una cadena de suministro de un Retail que puede ser visto
	Cerrada	Consortio	Restringido a un grupo autorizado de participantes	Participantes autorizados	Todos o una parte de los participantes autorizados	Múltiples bancos operando un registro compartido
		Privada y permisionada	Totalmente privado o restringido a un conjunto limitado de nodos autorizados	Solo el operados de la red	Solo el operados de la red	Libro mayor bancario externo compartido entre la empresa matriz y las subsidiarias

4. Tipos de Blockchain

Ernest & Young (EY) (2018). IFRS (#) Accounting for crypto-assets (EY). Disponible en: https://eyfinancialservicesthoughtgallery.ie/wp-content/uploads/2018/03/EY-IFRS-Accounting-for-crypto-assets.pdf

Witzig P., y Salomon V. (2018). CUTTING OUT THE MIDDLEMAN: A CASE STUDY OF BLOCKCHAIN-INDUCED RECONFIGURATIONS IN THE SWISS FINANCIAL SERVICES INDUSTRY (WORKING PAPER 1 – 2018/E, MAPS). Disponible en: http://www.unine.ch/files/live/sites/maps/files/shared/documents/wp/WP-1_2018_Witzig%20and%20Salomon.pdf

Si bien hay un gran número de características variables, dos de las más importantes son la apertura de la plataforma (público o privado) y el nivel de permiso requerido para añadir información a la Blockchain (permisionado o no permisionado)