2021-1-IE01-KA220-VET-000032943

Co-funded by the
Erasmus+ Programme
of the European Union

TrainChain
Blockchain Training for Start Ups

Contenido básico de PR1-T3

Módulo 0 — Introducción a la tecnología Blockchain

Autor del artículo: CCSDE

ID DEL PROYECTO:

Acuerdo de subvención	2021-1-IE01-KA220-VET-000032943
Programa	Erasmus+
Acción clave	KA220-VET — Asociaciones de cooperación en educación y formación profesionales
Campo	Educación y formación profesional
Acrónimo del proyecto	TrainChain
Título del proyecto	TrainChain — Blockchain Training for Start Ups
Fecha de inicio del proyecto	28/02/2022
Duración del proyecto	24 meses
Fecha de finalización del proyecto	27/02/2024

ser consideradas responsables del uso que pueda hacerse de la información contenida en las mismas.

HISTORIAL DE REVISIONES

Versión	Fecha	Autor	Descripción	Medidas de acción	Páginas
1.0	31/07/2022	CCSDE	Creación	C	8

(*) Acción: C = Creación, I = Insertar, U = Actualización, R = Reemplazar, D = Eliminar

DOCUMENTOS DE REFERENCIA

ID	Referencia		Título
1	2021-1-IE01-KA220-VET-000032943		Acuerdo de TrainChain
2			

DOCUMENTOS APLICABLES

ID	Referencia		Título
1			
2			

Contenido

1. Introducción

1.1 Descripción del módulo

En la primera parte del módulo, vamos a...

- Descubrir el nuevo mundo del blockchain.
- Entender por qué son importantes.

En la segunda parte del módulo, vamos a...

- Identificar los tres tipos de blockchains.
- Profundizar sobre cómo funciona el blockchain.

1.2 Objetivos del módulo

1.3 Objetivos de aprendizaje

1.4 Resultados de aprendizaje

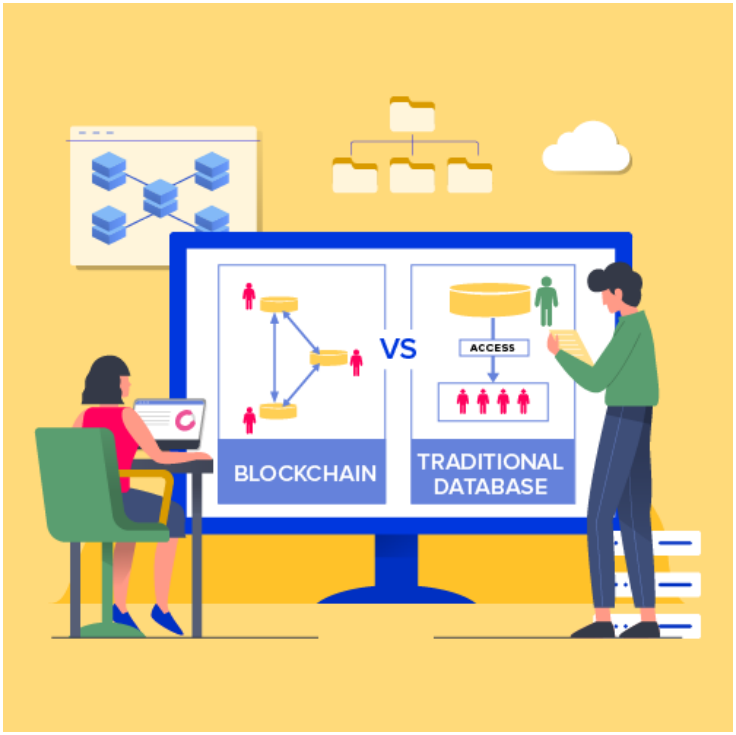
2. Contenido principal

2.1 Blockchain

Originalmente, blockchain era solo el término en ingeniería informática que se usaba para hacer referencia a cómo estructurar y compartir datos. Hoy en día, las cadenas de bloques se consideran la quinta evolución de la computación.

El blockchain es un enfoque novedoso sobre la base de datos distribuida. La innovación proviene de la incorporación de tecnología antigua de una forma nueva. Se puede pensar en las blockchains como bases de datos distribuidas que un grupo de individuos controla y que almacenan y comparten información.

Hay muchos tipos diferentes de blockchains y aplicaciones de blockchain. Blockchain es concretamente una tecnología amplia que se está integrando en plataformas y *hardware* en todo el mundo.



¿Qué son las blockchains?

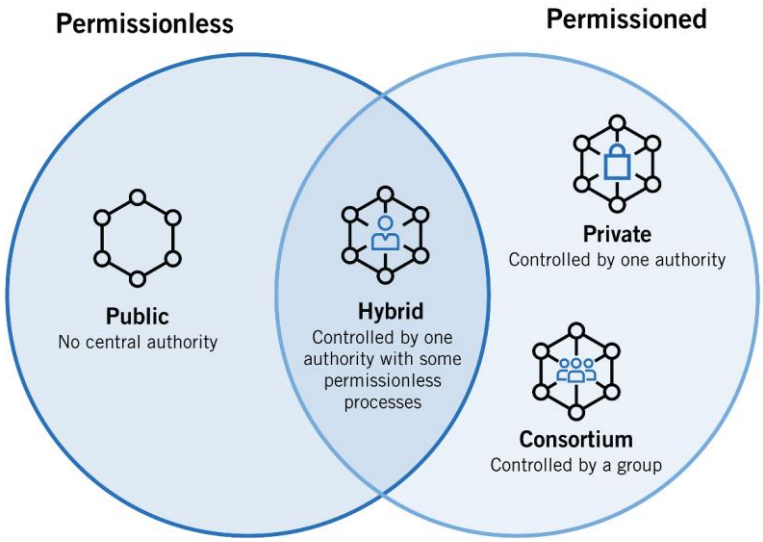
Una blockchain (o cadena de bloques, en español) es una estructura de datos que permite crear un libro de datos digital y compartirlo entre una red de partes independientes. Hay muchos tipos diferentes de blockchains:

- Cadenas de bloques públicas: las cadenas de bloques públicas, como Bitcoin, son grandes redes distribuidas que se ejecutan a través de una criptomoneda nativa. Una criptomoneda es un conjunto único de datos que se puede intercambiar entre dos partes. Las cadenas de bloques públicas están abiertas para que cualquier persona participe en cualquier nivel y tengan código de código abierto que mantiene su comunidad.

- Cadenas de bloques permisionadas: las blockchains permisionadas, como Ripple, controlan los roles que los individuos pueden desempeñar dentro de la red. Todavía son sistemas grandes y distribuidos que utilizan un token nativo. Su código central puede o no ser de código abierto.

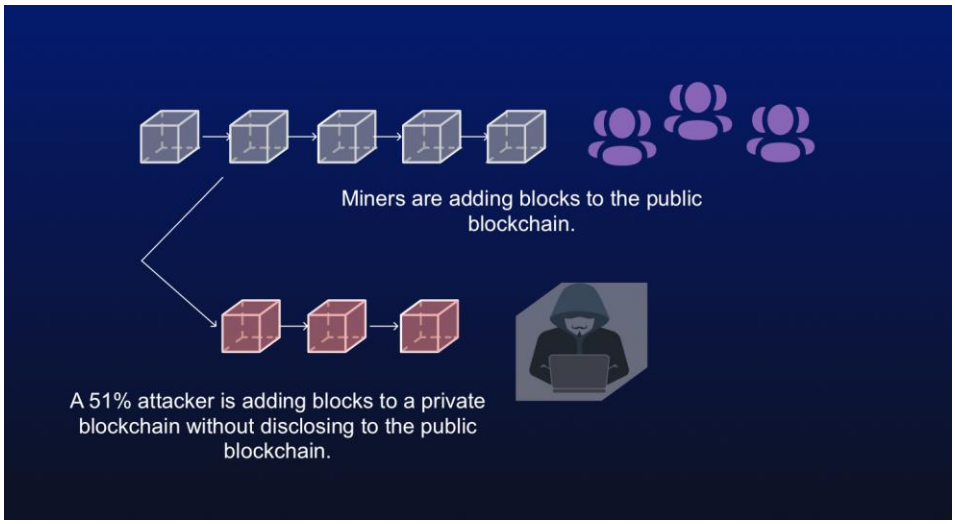
- Cadenas de bloques privadas: Las cadenas de bloques privadas también conocidas como tecnología de contabilidad distribuida (DLT) tienden a ser más pequeñas y no utilizan un token o criptomoneda. Su membresía está estrechamente controlada. Este tipo de blockchains son preferidas por consorcios que tienen miembros de confianza y comercian información confidencial.

Los tres tipos de blockchains utilizan criptografía para permitir que cada participante en una red dada administre el libro mayor de una manera segura sin la necesidad de una autoridad central para hacer cumplir las reglas. La eliminación de la autoridad central de la estructura de la base de datos es uno de los aspectos más importantes y poderosos de las cadenas de bloques.



Las cadenas de bloques crean registros permanentes e historiales de transacciones, pero nada es realmente permanente. La permanencia del registro se basa en la fiabilidad y salud de la red. En el contexto de las cadenas de bloques, esto significa que si una gran parte de la comunidad de blockchain quisiese cambiar la información escrita en su blockchain, podrían hacerlo. La criptomoneda se utiliza como recompensa para incentivar a muchos usuarios para facilitar la función saludable de la red a través de la competencia. Si los registros se cambian de manera inapropiada, esto se conoce como un ataque del 51 por ciento. Las redes pequeñas con pocos menores independientes son vulnerables porque no se necesita mucho esfuerzo para cambiar su

información, y los mineros poderosos podrían hacerlo y obtener criptomonedas adicionales.

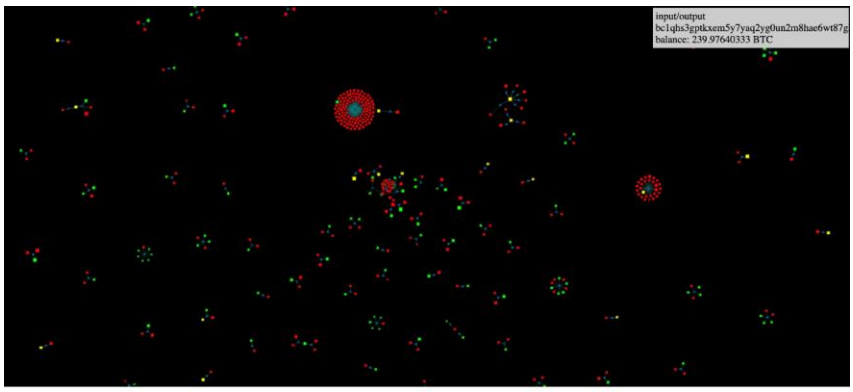


Lo que hacen las cadenas de bloques

Una cadena de bloques es un sistema *peer-to-peer* sin autoridad central que gestione el flujo de datos. Una de las formas clave de eliminar el control central mientras sin sacrificar la integridad de los datos es tener una gran red distribuida de usuarios independientes. Esto significa que los equipos que componen la red se encuentran en más de una ubicación. Estas computadoras a menudo se conocen como «nodos completos».

La Figura 1-1 muestra una visualización de la estructura de la red blockchain de Bitcoin. Puedes verlo en acción en http://dailyblockchain.github.io.

Commented [Ma1]: No se hace referencia a las cifras, y algunas de ellas son ilegibles



Para evitar que la red se corrompa, no solo se descentralizan las cadenas de bloques, sino que a menudo también utilizan una criptomoneda. Las redes blockchain producen criptomonedas como un incentivo para mantener la integridad de la red. Muchas criptomonedas se negocian en el mercado como acciones.

Las criptomonedas funcionan de manera un poco diferente en cada blockchain. Básicamente, el *software* paga el *hardware* para operar. El *software* es el protocolo blockchain. Los protocolos de blockchain más conocidos incluyen Bitcoin, Ethereum, Ripple, Bitcoin Cash, Stellar y EOS. El *hardware* consiste en los nodos completos que están asegurando los datos en la red.

¿Por qué importan las cadenas de bloques?

Las cadenas de bloques son reconocidas como la «quinta evolución» de la computación porque proporcionan una nueva capa de confianza para Internet. Antes de las cadenas de bloques, la confianza la establecían las autoridades centrales que emitían certificados. Uno con el que puede estar familiarizado es con los certificados de cliente Secure Sockets Layer (SSL), esto es el «candado verde» que está al lado de un dominio web que permite saber que estás en un sitio web seguro. Los certificados SSL han demostrado no ser infalibles, ya que ya han sido robados de los dominios de la Agencia Central de Inteligencia (CIA), el Servicio Secreto de Inteligencia del Reino Unido (comúnmente conocido como MI6), Microsoft, Yahoo!Skype, Facebook y Twitter. Confiar en un tercero significa que haya riesgo de fracaso.

Las cadenas de bloques, por otro lado, establecen la confianza de maneras novedosas. Las cadenas de bloques de sistema de prueba de trabajo (POW — *proof of* work en inglés) requieren que los mineros tengan un historial completo y preciso de sus transacciones para participar en la red. Las cadenas de bloques de prueba de participación (POS, por sus siglas en inglés) crean confianza al requerir que los nodos que están procesando transacciones «tomen» alguna criptomoneda que puede perderse si se les detecta defraudando a la red. Las cadenas de bloques privadas crean confianza mediante la distribución de datos a través de una red de participantes conectados pero independientes que se conocen entre sí y que pueden rendirse cuentas. Cada tipo de blockchain utiliza diferentes sistemas de incentivos para establecer la confianza de que los participantes en la red cooperarán para mantener un historial completo e inalterado de cada transacción o entrada que se realiza dentro de la base de datos que comparten.

Cuando los datos son permanentes y fiables en un formato digital, se pueden realizar transacciones de negocios en línea de maneras que, en el pasado, solo eran posibles *offline*. Todo lo que hasta ahora ha permanecido análogo, incluidos los derechos de propiedad y la identidad, ahora se puede crear y mantener en línea. Los procesos comerciales y bancarios lentos, como transferencias de dinero y liquidaciones de fondos, ahora se pueden hacer casi instantáneamente. Las implicaciones de los registros digitales seguros son enormes para la economía global.

Las cadenas de bloques son importantes porque permiten una nueva eficiencia y fiabilidad en el intercambio de información valiosa y privada que antes requería que un tercero facilitara, como el movimiento de dinero y la autenticidad de la identidad. Esto es importante porque gran parte de nuestra sociedad y economía se ha estructurado en torno al establecimiento de confianza, la imposición de la confianza cuando se rompe, y terceros que facilitan la confianza. Se puede imaginar cómo se puede utilizar blockchain para arreglar áreas que han demostrado no ser infalibles, como el voto, la gestión de la cadena de suministro, el movimiento de dinero y el intercambio de propiedades.

La Estructura de Blockchains

Cada cadena de bloques está estructurada de manera ligeramente diferente. Sin embargo, Bitcoin es una gran cadena de bloques que estudiar porque se utilizó como plantilla para la mayoría de las cadenas de bloques posteriores. Los datos sobre Bitcoin están estructurados de modo que cada nodo completo (los equipos que ejecutan la red) contenga todos los datos de la red. Este modelo es convincente desde el punto de vista de la persistencia de los datos, ya que asegura que los datos permanecerán intactos incluso si algunos de los nodos se ven comprometidos. Sin embargo, debido a

que cada nodo tiene una copia completa del historial de transacciones, desde el principio, y cada transacción futura, requiere que las entradas sean lo más pequeñas posible desde el punto de vista de la capacidad de almacenamiento.

De forma comparativa, otras redes distribuidas de las que puede haber oído hablar como Napster y Pirate Bay son un índice de datos en línea. Los archivos individuales se comparten desde nodos específicos de la red, lo cual permite compartir archivos grandes. Sin embargo, debido a que los datos que te pueden interesar no están disponibles en todos los participantes de la red, obtener los datos que te interesan es problemático. También es difícil saber si los datos están intactos, no se han corrompido o si contienen información que no se desea, como un virus.

La forma en que Bitcoin coordina la organización y la entrada de nuevos datos comprende tres elementos centrales:

1. **Bloque**: Una lista de las transacciones registradas en un libro mayor durante un período determinado. El tamaño, el período y el evento desencadenante de los bloques es diferente para cada blockchain.

No todas las cadenas de bloques registran y aseguran un registro del movimiento de su criptomoneda como objetivo principal, pero todas registran el movimiento de su criptomoneda o token. Piensa en la transacción como simplemente el registro de datos. Asignarle un valor (como sucede en una transacción financiera) se utiliza para interpretar lo que significan esos datos.

2. **Cadena**: Un *hash* que vincula un bloque a otro, encadenándolos matemáticamente. Este es uno de los conceptos más difíciles de comprender en blockchain. También es la «magia» que pega blockchains y les permite crear confianza matemática.

El *hash* en blockchain se crea a partir de los datos que estaban en el bloque anterior. Es decir, es una huella dactilar de estos datos que además bloquea los bloques en orden y tiempo.

Aunque las cadenas de bloques son una innovación relativamente nueva, lo que se conoce como *hashing* no lo es, ya que fue inventado hace más de 30 años. Esta vieja innovación se está utilizando porque crea una función unidireccional que no se puede descifrar. Una función de hashing crea un algoritmo matemático que asigna datos de cualquier tamaño a una cadena de bits de un tamaño fijo. Una cadena de bits suele ser de 32 caracteres de largo, que luego representa los datos que se registraron con el hashing. El Algoritmo de Hash Seguro (SHA) es una de las funciones *hash* criptográficas utilizadas en blockchains. Sha-256 es un algoritmo común que genera un *hash* casi único de un tamaño fijo de 256 bits (32 bytes). Con fines prácticos, piense en un *hash* como una huella digital de datos que se utiliza para bloquearla en su lugar dentro de la cadena de bloques.

3. **Red**: La red está compuesta por nodos completos. Piensa en ellos como el equipo que ejecuta un algoritmo que está asegurando la red. Cada nodo contiene un registro completo de todas las transacciones que se registraron en esa cadena de bloques.

Los nodos se encuentran en todo el mundo y pueden ser operados por cualquier persona. Es difícil, costoso y lleva mucho tiempo operar un nodo completo, por lo que las personas están incentivadas a operar un nodo porque a cambio ganan criptomonedas. Por su servicio, el algoritmo blockchain subyacente les da una recompensa, que suele ser un token o una criptomoneda, como Bitcoin.

2.2 Principales Aplicaciones y Evolución del Blockchain

Las aplicaciones blockchain se construyen en torno a la idea de que la red es el árbitro. Este tipo de sistema es un entorno implacable y ciego. El código informático se convierte en ley, y las reglas se ejecutan como fueron escritas e interpretadas por la red. Los equipos no tienen los mismos sesgos y comportamientos sociales que los humanos.

La red no puede interpretar la intención (al menos todavía). Los contratos de seguros arbitrados en una cadena de bloques han sido fuertemente investigados como un caso de uso construido en torno a esta idea.

Otra cosa interesante que permiten las cadenas de bloques es el mantenimiento impecable de registros. Se pueden utilizar para crear una línea de tiempo clara de quién hizo qué y cuándo. Muchas industrias y organismos reguladores pasan incontables horas tratando de evaluar este problema. El mantenimiento de registros habilitado por blockchain aliviará algunas de las cargas que se crean cuando tratamos de interpretar el pasado.

El ciclo de vida de Blockchain

Las cadenas de bloques se originaron con la creación de Bitcoin. Esto demostró que un grupo de personas que nunca se habían reunido podían operar en línea dentro de un sistema que estaba insensibilizado para engañar a otros que cooperaban en la red.

La red original de Bitcoin fue construida para asegurar la criptomoneda Bitcoin. Tiene alrededor de 5.000 nodos completos y se distribuye globalmente. Se utiliza principalmente para comerciar con Bitcoin y el valor de intercambio, pero la comunidad vio el potencial de hacer mucho más con la red. Debido a su tamaño y seguridad probada en el tiempo, también se está utilizando para proteger otras blockchains y aplicaciones de blockchain más pequeñas.

La red Ethereum es una segunda evolución del concepto blockchain. Toma la estructura tradicional de blockchain y agrega varios lenguajes nuevos de programación que se construyen dentro de ella. Al igual que Bitcoin, tiene más de 10.000 nodos completos y se distribuye globalmente. Ethereum se utiliza principalmente para comerciar con Ether y crear contratos inteligentes o *smart contracts*. El contrato inteligente más popular de Ethereum es el ERC 20, que permite la generación de tokens intercambiables. Estos tokens se pueden utilizar para fines de recaudación de fondos.

Hay una tercera evolución en la tecnología blockchain que está en desarrollo activo y aborda las restricciones de velocidad y tamaño de los datos. Solucionar estos problemas permitirá que la tecnología blockchain se utilice de manera más realista con aplicaciones convencionales. Llevará varios años que quede claro qué estructura ganará.

Los nuevos desarrollos populares incluyen el *sharding*, un tipo de partición de bases de datos que separa grandes bases de datos en partes más pequeñas llamadas fragmentos de datos. Un esfuerzo de desarrollo de Ethereum llamado regla de elección de bifurcación divide la cadena de bloques Ethereum en varias redes paralelas. Esto puede permitir una escalabilidad de Ethereum más eficiente y una reducción de la congestión en la red, aumentando así las velocidades de transacción y reduciendo los costos de transacción.

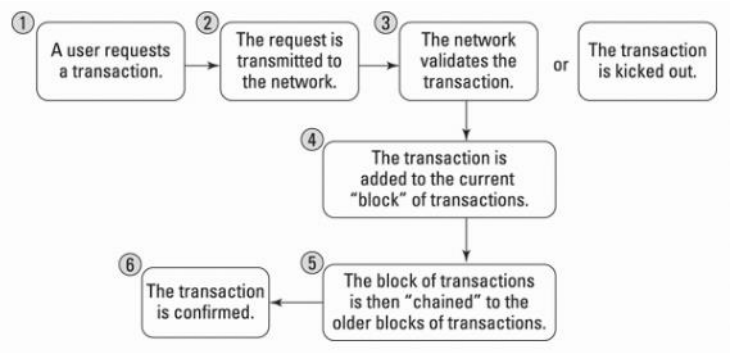
Otra teoría de escala popular se llama POS. En términos generales, el POS es el concepto de poner tokens o criptomonedas como un bono para procesar transacciones. Si el nodo está dañado y no procesa las transacciones con precisión, puede perder sus tokens o criptomonedas.

Un tercer esfuerzo para escalar la tecnología blockchain utiliza nodos de confianza. Por ejemplo, la red Factom opera con nodos federados y un número ilimitado de nodos de auditoría. Se confía en estos nodos para garantizar el sistema. La red elegida de Factom es pequeña, con poco más de 60 nodos. Para cubrir los riesgos de seguridad, Factom se ancla en otras redes distribuidas para aprovechar la seguridad de sistemas más extensos. Factom también divide su red en partes más pequeñas, más rápidas y más fáciles de manejar llamadas cadenas. Factom tiene velocidades de transacción más rápidas y costos de transacción más bajos que las cadenas de bloques POW.

Consenso: La fuerza impulsora de las cadenas de bloques

Las cadenas de bloques son herramientas poderosas porque crean sistemas honestos que se corrigen por sí mismos sin la necesidad de un tercero para hacer cumplir las reglas. Logran la aplicación de las reglas a través de su algoritmo de consenso.

En el mundo blockchain, el consenso es el proceso de desarrollar un acuerdo entre un grupo de accionistas comúnmente desconfiados. Estos son los nodos completos de la red. Los nodos completos validan las transacciones que se ingresan en la red y que se registrarán como parte del libro mayor.



Cada blockchain tiene sus propios algoritmos para crear un acuerdo dentro de su red sobre las entradas que se agregan. Hay muchos modelos diferentes para crear consenso porque cada blockchain crea diferentes tipos de entradas. Algunas cadenas de bloques son de valor comercial, otras almacenan datos, y otras aseguran sistemas y contratos.

Bitcoin, por ejemplo, está negociando el valor de su token entre los miembros de su red. Los tokens tienen un valor de mercado, por lo que los requisitos relacionados con el rendimiento, la escalabilidad, la consistencia, el modelo de amenaza y el modelo de fallo serán más altos. Bitcoin opera bajo el supuesto de que un atacante malicioso puede querer corromper la historia de las operaciones con el fin de robar tokens. Bitcoin evita que esto suceda mediante el uso de un modelo de consenso llamado «prueba de trabajo» (*proof-of-work*, en inglés) que resuelve el problema del general bizantino: «¿Cómo sabes que la información que estás viendo no se ha cambiado internamente o externamente?» Debido a que cambiar o manipular datos casi siempre es posible, la fiabilidad de los datos es un gran problema para la informática.

La mayoría de las cadenas de bloques operan bajo la premisa de que serán atacadas por fuerzas externas o por usuarios del sistema. La amenaza esperada y el grado de confianza que la red tiene en los nodos que operan la cadena de bloques determinará el tipo de algoritmo de consenso que utilizan para liquidar su libro mayor. Por ejemplo, Bitcoin y Ethereum esperan un grado muy alto de amenaza y utilizan un algoritmo de consenso fuerte llamado prueba de trabajo. No hay confianza en la red.

En el otro extremo del espectro, las cadenas de bloques que se utilizan para registrar transacciones financieras entre partes conocidas pueden usar un consenso más ligero y rápido. La necesidad de efectuar transacciones de alta velocidad es más importante. El sistema de prueba de trabajo es demasiado lenta y costosa en este caso, debido a los pocos participantes dentro de la red en comparación con otras y la necesidad inmediata de finalización para cada transacción. Tampoco necesitan un token o

criptomoneda para incentivar el procesamiento de transacciones. Por lo tanto, eliminan estos elementos de su sistema y funcionan más rápido y más barato que los sistemas POW.

2.3 Usos de otras tecnologías Blockchain

Hoy en día, existen miles de blockchains y aplicaciones de blockchain. Todo el mundo se ha obsesionado con las ideas de mover dinero más rápido, incorporar y gobernar en una red distribuida, y construir aplicaciones y hardware seguros.

Puedes ver muchas de estas cadenas de bloques públicas yendo a un intercambio de criptomonedas.

La siguiente figura muestra el intercambio de altcoin para Poloniex (https://poloniex.com), una plataforma de comercio de criptomonedas.

Las cadenas de bloques se están moviendo más allá del mercado de valor comercial y se están incorporando a todo tipo de industrias. Las cadenas de bloques agregan una nueva capa de confianza que ahora hace que trabajar en línea sea seguro de una manera que no era posible de antemano.

Usos actuales de blockchain

La mayoría de las aplicaciones blockchain en funcionamiento giran en torno a mover dinero u otras formas de valor de forma rápida y barata. Esto incluye el comercio de acciones de la empresa pública, el pago de empleados en otros países, y el intercambio de una moneda por otra.

Las cadenas de bloques también se están utilizando ahora como parte de una pila de seguridad de software. El Departamento de Seguridad Nacional de los Estados Unidos ha estado investigando el software blockchain que protege los dispositivos que usan el Internet de las Cosas (IoT). El mundo del IoT obtiene algunos de los mayores beneficios de esta tecnología innovadora, porque es especialmente vulnerable a la suplantación y otras formas de hackeo. Los dispositivos IoT también se han vuelto más omnipresentes, y la seguridad se ha vuelto más dependiente de ellos. Los sistemas hospitalarios, los automóviles autónomos y los sistemas de seguridad son los principales ejemplos.

Las Ofertas de Monedas Iniciales (ICO) son otra innovación emocionante de blockchain. Son un tipo de contrato inteligente que permite al emisor ofrecer un token a cambio de fondos de inversión. A menudo utilizados como una opción de recaudación de fondos no dilutiva, gracias a esto, los empresarios a nivel mundial han podido recaudar miles de millones de dólares. Los gobiernos y los reguladores se han apresurado a tomar medidas contra las ICO. Los tokens pueden ser valores sin licencia, y la oferta puede estar defraudando a los inversores. La tecnología es impresionante incluso aunque todavía se estén abordando problemas de cumplimiento.

Una de las innovaciones fantásticas inherentes a los tokens ICO es que son un instrumento autolimpiable y autoestablecido. En nuestro sistema actual de negociación de valores, hay dos tipos de agencias de compensación: empresas de compensación y depositarios. Las empresas compensadoras auditan las transacciones y actúan como intermediarios en la liquidación, mientras que los depositarios poseen certificados de valores y mantienen registros de propiedad de los valores. Las cadenas de bloques realizan ambas funciones para los tokens sin necesidad de que terceros auditen y conserven la posesión de los activos.

Futuras aplicaciones de blockchain

Los proyectos de blockchain más grandes y de mayor duración que se están explorando ahora incluyen sistemas de registro de tierras respaldados por el gobierno, identidad y aplicaciones de seguridad de viajes internacionales.

Las posibilidades de un futuro infundido en blockchain han motivado la imaginación de los empresarios, gobiernos, grupos políticos y humanitarios en todo el mundo. Países como el Reino Unido, Singapur y los Emiratos Árabes Unidos lo ven como una forma de reducir costos, crear nuevos instrumentos financieros y mantener registros limpios. Además, tienen inversiones e iniciativas activas que exploran la tecnología blockchain.

Las cadenas de bloques han sentado una base donde la necesidad de confianza se ha eliminado de la ecuación. Antes pedir «confianza» era un gran problema pero con blockchains deja de serlo. Además, la infraestructura que hace cumplir la regla si esa confianza se rompe puede ser mucho más ligera. Dado que gran parte de la sociedad se basa en la confianza y el cumplimiento de las normas, las implicaciones sociales y económicas de las aplicaciones blockchain pueden ser emocional y políticamente

polarizadoras. Blockchain cambiará la forma en que estructuramos transacciones basadas en valores y basadas en la sociedad.

3. Evaluación del conocimiento

4. Resumen del módulo

5. Referencias