BLOCKCHAIN EXPLICADO

ACCELERALIA
acceleration platform

BLOCKCHAIN EXPLICADO

Si ha estado siguiendo la banca, la inversión o las criptomonedas durante los últimos diez años, es posible que esté familiarizado con "blockchain", la tecnología de mantenimiento de registros detrás de la red Bitcoin. Y hay una buena posibilidad de que tenga mucho sentido. Al tratar de aprender más sobre blockchain, probablemente haya encontrado una definición como esta: "blockchain es un libro mayor público distribuido, descentralizado".
La buena noticia es que blockchain es en realidad más fácil de entender de lo que suena esa definición.

¿Qué es el Blockchain?

Si esta tecnología es tan compleja, ¿por qué llamarla "blockchain"? En su nivel más básico, blockchain es literalmente solo una cadena de bloques, pero no en el sentido tradicional de esas palabras. Cuando decimos las palabras "bloque" y "cadena" en este contexto, en realidad estamos hablando de información digital (el "bloque") almacenada en una base de datos pública (la "cadena").
Los "bloques" en la cadena de bloques se componen de piezas digitales de información. Específicamente, tienen tres partes:

Bloquea la información de la tienda sobre transacciones como la fecha, la hora y el monto en dólares de su compra más reciente en Amazon.
(NOTA: Este ejemplo de Amazon es para compras ilustrativas; el comercio minorista de Amazon no funciona en un principio de cadena de bloques al momento de escribir este artículo)
Los bloques almacenan información sobre quién participa en las transacciones. Un bloque para su compra derrochadora de Amazon registraría su nombre junto con Amazon.com, Inc. (AMZN). En lugar de usar su nombre real, su compra se registra sin ninguna información de identificación utilizando una "firma digital" única, algo así como un nombrede usuario.
Los bloques almacenan información que los distingue de otros bloques. Al igual que tú y yo tenemos nombres para distinguirnos entre nosotros, cada bloque almacena un código único llamado "hash" que nos permite diferenciarlo de todos los demás bloques. Los hash son códigos criptográficos creados por algoritmos especiales. Supongamos que hizo su compra derrochadora en Amazon, pero mientras está en tránsito, decide que no puede resistirse y necesita una segunda. Aunque los detalles de su nueva transacción se verían casi idénticos a los de su compra anterior, aún podemos diferenciar los bloques debido a sus códigos únicos.
Si bien el bloque del ejemplo anterior se usa para almacenar una sola compra de Amazon, la realidad es un poco diferente. Un solo bloque en la cadena de bloques de Bitcoin puede almacenar alrededor de 1 MB de datos.1 Dependiendo del tamaño de las transacciones, eso significa que un solo bloque puede albergar varios miles de transacciones bajo un mismo techo.

Cómo funciona Blockchain

1. Cuando un bloque almacena nuevos datos, se agrega a la cadena de bloques. Blockchain, como su nombre indica, consta de varios bloques unidos. Sin embargo, para que se agregue un bloque a la cadena de bloques, deben suceder cuatro cosas:

Debe ocurrir una transacción. Continuemos con el ejemplo de su compra impulsiva en Amazon. Después de hacer clic apresuradamente en varios mensajes de pago, va en contra de su mejor criterio y realiza una compra. Como discutimos anteriormente, en muchos casos un bloque agrupará po-

tencialmente miles de transacciones, por lo que su compra de Amazon se empaquetará en el bloque junto con la información de la transacción de otros usuarios también.

2. Esa transacción debe ser verificada. Después de realizar esa compra, su transacción debe ser verifi- cada. Con otros registros públicos de información, como la Comisión de Bolsa de Valores, Wikipedia osu biblioteca local, hay alguien a cargo de examinarlas nuevas entradas de datos. Sin embargo, con blockchain, ese trabajo se deja en manos de una red de computadoras. Cuando realiza su compra en Amazon, esa red de computadoras se apresura a verificar que su transacción sucedió de la manera que dijo que sucedió. Es decir, confirman los deta- lles de la compra, incluido el tiempo de la transac- ción, el monto en dólares y los participantes. (Más sobre cómo sucede esto en un segundo).

3. Esa transacción debe almacenarse en un bloque. Una vez que su transacción ha sido verificada como precisa, recibe luz verde. El monto en dólares de la transacción, su firma digital y la firma digital de Amazon se almacenan en un bloque. Allí, la transacción probablemente se unirá a cientos o miles de otras similares.

4. A ese bloque se le debe asignar un hash. Al igual que un ángel que se gana las alas, una vez que se han verificado todas las transacciones de un bloque, se le debe dar un código de identificación único llamado hash. El bloque también recibe el hash del bloque más reciente agregado a la cadena de bloques. Una vez procesado, el bloque se puede agregar a la cadena de bloques.

Cuando ese nuevo bloque se agrega a la cadena de bloques, se pone a disposición del público para que cualquiera lo vea, incluso usted. Si echas un vistazo a la cadena de bloques de Bitcoin, verás que tienes acceso a los datos de la transacción, junto con información sobre cuándo ("Hora"), dónde ("Altura") y quién ("Retransmitido por") fue el bloque. agregado a la cadena de bloques.

¿Blockchain es privado?

Cualquiera puede ver el contenido de la cadena de bloques, pero los usuarios también pueden optar por conectar sus computadoras a la red de la cadena de bloques como nodos. Al hacerlo, su computadora recibe una copia de la cadena de bloques que se actualiza automáticamente cada vez que se agrega un nuevo bloque, algo así como una fuente de noticias de Facebook que brinda una actualización en vivo cada vez que se publica un nuevo estado.

Cada computadora en la red blockchain tiene su propia copia de blockchain, lo que significa que hay miles, o en el caso de Bitcoin, millones de copias de la misma cadena de bloques. Aunque cada copia de la cadena de bloques es idéntica, difundir esa información a través de una red de computadoras hace que la información sea más difícil de manipular. Con blockchain, no hay una sola cuenta definitiva de eventos que se pueda manipular. En cambio, un pirata informático necesitaría manipular cada copia de la cadena de bloques en la red. Esto es lo que se entiende por blockchain como un libro mayor "distribuido".

Sin embargo, al mirar la cadena de bloques de Bitcoin, notará que no tiene acceso a la información de identificación sobre los usuarios que realizan transacciones. Aunque las transacciones en la cadena de bloques no son completamente anónimas, la información personal sobre los usuarios se limita a su firma digital o nombre de usuario.
Esto plantea una pregunta importante: si no puede saber quién está agregando bloques a la cadena de bloques, ¿cómo puede confiar en la cadena de bloques o en la red de computadoras que la sustenta?

¿Blockchain es seguro?

La tecnología Blockchain da cuenta de los problemas de seguridad y confianza de varias maneras.
Primero, los bloques nuevos siempre se almacenan de forma lineal y cronológica. Es decir, siempre se agregan al "final" de la cadena de bloques. Si echas un vistazo a la cadena de bloques de Bitcoin, verás que cada bloque tiene una posición en la cadena, llamada "altura". En agosto de 2020, la altura del bloque había superado los 646.132,2
Después de que se ha agregado un bloque al final de la cadena de bloques, es muy difícil volver atrás y alterar el contenido del bloque. Eso es porque cada bloque contiene su propio hash, junto con el hash del bloque anterior. Los códigos hash se crean mediante una función matemática que convierte la información digital en una cadena de números y letras. Si esa información se edita de alguna manera, el código hash también cambia.

He aquí por qué eso es importante para la seguridad. Supongamos que un pirata informático intenta editar su transacción desde Amazon para que realmente tenga que pagar su compra dos veces. Tan pronto como editen el monto en dólares de su transacción, el hash del bloque cambiará. El siguiente bloque de la cadena aún contendrá el hash antiguo, y el hacker necesitaría actualizar ese bloque para cubrir sus huellas. Sin embargo, hacerlo cambiaría el hash de ese bloque. Y el siguiente, y así sucesivamente.

Entonces, para cambiar un solo bloque, un pirata informático necesitaría cambiar cada bloque después de él en la cadena de bloques. Recalcular todos esos hashes requeriría una enorme e improbable cantidad de poder de cómputo. En otras palabras, una vez que se agrega un bloque a la cadena de bloques, se vuelve muy difícil de editar e imposible de eliminar.

Para abordar el tema de la confianza, las redes blockchain han implementado pruebas para las computadoras que desean unirse y agregar bloques a la cadena. Las pruebas, llamadas "modelos de consenso", requieren que los usuarios se "prueben" a sí mismos antes de poder participar en una red blockchain. Uno de los ejemplos más comunes empleados por Bitcoin se llama "prueba de trabajo".

En el sistema de prueba de trabajo, las computadoras deben "probar" que han hecho "trabajo" resolviendo un problema matemático computacional complejo. Si una computadora resuelve uno de estos problemas, será elegible para agregar un bloque a la cadena de bloques. Pero el proceso de agregar bloques a la cadena de bloques, lo que el mundo de las criptomonedas llama "minería", no es fácil. De hecho, las probabilidades de resolver uno de estos problemas en la red de Bitcoin eran aproximadamente de uno en 17.56 billones en agosto de 2020.2 Para resolver problemas matemáticos complejos con esas probabilidades, las computadoras deben ejecutar programas que les cuestan cantidades significativas de energía.

La prueba de trabajo no imposibilita los ataques de los piratas informáticos, pero los hace algo inútiles. Si un pirata informático quisiera coordinar un ataque a la cadena de bloques, necesitaría controlar más del 50% de toda la potencia informática en la cadena de bloques para poder abrumar a todos los demás participantes en la red. Dado el tremendo tamaño de la cadena de bloques de Bitcoin, es casi seguro que un ataque del 51% no valga la pena el esfuerzo y es más que probable que sea imposible.

Blockchain vs. Bitcoin

El objetivo de blockchain es permitir que la información digital se registre y distribuya, pero no se edite. Ese concepto puede ser difícil de entender sin ver la tecnología en acción, así que echemos un vistazo a cómo funciona realmente la primera aplicación de la tecnología blockchain.
La tecnología Blockchain fue esbozada por primera vez en 1991 por Stuart Haber y W. Scott Stornetta, dos investigadores que querían implementar un sistema donde las marcas de tiempo de los documentos no pudieran ser manipuladas.3 Pero no fue hasta casi dos décadas después, con el lanzamiento de Bitcoin en enero de 2009, esa cadena de bloques tuvo su primera aplicación en el mundo real. El protocolo Bitcoin se basa en la cadena de bloques. En un correo electrónico que anunciaba su trabajo de investigación sobre la introducción de la moneda digital, el creador seudónimo de Bitcoin, Satoshi Nakamoto, se refirió a ella como "un nuevo sistema de efectivo electrónico que es totalmente peer-to-peer, sin un tercero de confianza".

Así es como funciona.

Tienes a todas estas personas, en todo el mundo, que tienen bitcoins. Es probable que haya muchos millones de personas en todo el mundo que posean al menos una parte de un bitcoin. Digamos que uno de esos millones de personas quiere gastar sus bitcoins en comestibles. Aquí es donde entra la cadena de bloques.

Cuando se trata de dinero impreso, el uso de moneda impresa está regulado y verificado por una autoridad central, generalmente un banco o un gobierno, pero Bitcoin no está controlado por nadie. En cambio, las transacciones realizadas en bitcoin son verificadas por una red de computadoras. Esto es lo que significa que la red Bitcoin y la cadena de bloques están "descentralizadas".

Cuando una persona paga a otra por bienes usando bitcoin, las computadoras en la red Bitcoin compiten para verificar la transacción. Para hacerlo, los usuarios ejecutan un programa en sus computadoras e intentan resolver un problema matemático complejo, llamado "hash". Cuando una computadora resuelve el problema mediante el "hash" de un bloque, su trabajo algorítmico también habrá verificado las transacciones del bloque. Como des-

cribimos anteriormente, la transacción completada se registra públicamente y se almacena como un bloque en la cadena de bloques, momento en el que se vuelve inalterable. En el caso de Bitcoin y la mayoría de las otras cadenas de bloques, las computadoras que verifican con éxito los bloques son recompensadas por su trabajo con criptomonedas. Esto se conoce comúnmente como "minería".

Aunque las transacciones se registran públicamente en la cadena de bloques, los datos del usuario no lo están, o al menos no en su totalidad. Para realizar transacciones en la red Bitcoin, los participantes deben ejecutar un programa llamado "billetera". Cada billetera consta de dos claves criptográficas únicas y distintas: una clave pública y una clave privada. La clave pública es la ubicación donde se depositan y retiran las transacciones. Esta es también la clave que aparece en el libro mayor de blockchain como la firma digital del usuario.

Incluso si un usuario recibe un pago en bitcoins a su clave pública, no podrá retirarlos con la contraparte privada. La clave pública de un usuario es una versión abreviada de su clave privada, creada mediante un complicado algoritmo matemático. Sin embargo, debido a la complejidad de esta ecuación, es casi imposible revertir el proceso y generar una clave privada a partir de una clave pública. Por esta razón, la tecnología blockchain se considera confidencial.

Conceptos básicos de claves públicas y privadas

Aquí está la versión ELI5: "Explíquelo como si tuviera 5 años". Puede pensar en una clave pública como un casillero de la escuela y la clave privada como la combinación del casillero. Los profesores, los estudiantes e incluso la persona que te gusta pueden insertar letras y notas a través de la abertura de tu casillero. Sin embargo, la única persona que puede recuperar el contenido del buzón es la que tiene la clave única. Sin embargo, debe tenerse en cuenta que, si bien las combinaciones de casilleros escolares se guardan en la oficina del director, no existe una base de datos central que realice un seguimiento de las claves privadas de una red blockchain. Si un usuario extravía su clave privada, perderá el acceso a su billetera bitcoin, como fue el caso de este hombre que llegó a los titulares nacionales en diciembre de 2017.

Una sola cadena pública

En la red Bitcoin, la cadena de bloques no solo es compartida y mantenida por una red pública de usuarios, sino que también se acuerda. Cuando los usuarios se unen a la red, su computadora conectada recibe una copia de la cadena de bloques que se actualiza cada vez que se agrega un nuevo bloque de transacciones. Pero, ¿qué pasa si, a través de un error humano o los esfuerzos de un pirata informático, la copia de un usuario de la cadena de bloques se manipula para que sea diferente de cualquier otra copia de la cadena de bloques?
El protocolo blockchain desalienta la existencia de múltiples blockchains a través de un proceso llamado "consenso". En presencia de copias múltiples y diferentes de la cadena de bloques, el protocolo de consenso adoptará la cadena más larga disponible. Más usuarios en una cadena de bloques significa que los bloques se pueden agregar al final de la cadena más rápido. Según esa lógica, la cadena de bloques de registro siempre será en la que confíen la mayoría de los usuarios. El protocolo de consenso es una de las mayores fortalezas de la tecnología blockchain, pero también permite una de sus mayores debilidades.

Teóricamente, a prueba de hackers

En teoría, es posible que un hacker se aproveche de la regla de la mayoría en lo que se conoce como un ataque del 51%. Así es como sucedería. Digamos que hay cinco millones de computadoras en la red de Bitcoin, una gran subestimación sin duda, pero un número bastante fácil de dividir. Para lograr la mayoría en la red, un pirata informático necesitaría controlar al menos 2,5 millones y una de esas computadoras. Al hacerlo, un atacante o un grupo de atacantes podría interferir con el proceso de registro de nuevas transacciones. Podían enviar una transacción y luego revertirla, haciendo que pareciera que todavía tenían la moneda que acababan de gastar. Esta vulnerabilidad, conocida como doble gasto, es el equivalente digital de una falsificación perfecta y permitiría a los usuarios gastar sus bitcoins dos veces.

Un ataque de este tipo es extremadamente difícil de ejecutar para una cadena de bloques de la escala de Bitcoin, ya que requeriría que un atacante obtuviera el control de millones de computadoras. Cuando Bitcoin se fundó por primera vez en 2009 y sus usuarios se contaban por docenas, habría sido más fácil para un atacante controlar la mayor parte de la potencia computacional en la red. Esta característica definitoria de blockchain se ha señalado como una debilidad de las criptomonedas incipientes.

El miedo de los usuarios a los ataques del 51% en realidad puede limitar la formación de monopolios en la cadena de bloques. En "Digital Gold: Bitcoin y la historia interna de los inadaptados y millonarios que intentan reinventar el dinero", el periodista del New York Times Nathaniel Popper escribe sobre cómo un grupo de usuarios, llamado "Bitfury", reunió miles de computadoras de alta potencia para obtener ganancias. una ventaja competitiva en blockchain. Su objetivo era extraer tantos bloques como fuera posible y ganar bitcoins, que en ese momento estaban valorados en aproximadamente $ 700 cada uno.

Aprovechando Bitfury

Sin embargo, en marzo de 2014, Bitfury se posicionó para superar el 50% de la potencia computacional total de la red blockchain. En lugar de seguir aumentando su control sobre la red, el grupo eligió autorregularse y prometió no superar nunca el 40%. Bitfury sabía que si optaban por continuar aumentando su control sobre la red, el valor de bitcoin caería a medida que los usuarios vendieran sus monedas en preparación para la posibilidad de un ataque del 51%. En otras palabras, si los usuarios pierden su fe en la red blockchain, la información en esa red corre el riesgo de volverse completamente inútil. Los usuarios de Blockchain, entonces, solo pueden aumentar su poder computacional hasta un punto antes de que comiencen a perder dinero.

Aplicación práctica de Blockchain

Los bloques en la cadena de bloques almacenan datos sobre transacciones monetarias; lo hemos sacado del camino. Pero resulta que blockchain es en realidad una forma bastante confiable de almacenar datos sobre otros tipos de transacciones. De hecho, la tecnología blockchain se puede utilizar para almacenar datos sobre intercambios de propiedades, paradas en una cadena de suministro e incluso votar por un candidato.

Deloitte encuestó recientemente a más de 1.400 empresas en 14 regiones sobre la integración de blockchain en sus operaciones. La encuesta encontró que el 82% de los encuestados planeaba contratar personal con blockchain
experiencia en los próximos 12 meses, y el 39% ya tenía un sistema blockchain en producción hoy. Además, el 36% de las empresas dijeron que invertirían $ 5 millones o más en blockchain el próximo año. Estas son algunas de las aplicaciones más populares de blockchain que se están explorando en la actualidad.

Uso bancario

Quizás ninguna industria se beneficie más de la integración de blockchain en sus operaciones comerciales que la banca. Las instituciones financieras solo operan durante el horario comercial, cinco días a la semana. Eso significa que si intenta depositar un cheque el viernes a las 6 p.m., probablemente tendrá que esperar hasta el lunes por la mañana para ver que el dinero llegue a su cuenta. Incluso si realiza su depósito durante el horario comercial, la transacción puede demorar de uno a tres días en verificar debido al gran volumen de transacciones que los bancos deben liquidar. Blockchain, por otro lado, nunca duerme.

Al integrar blockchain en los bancos, los consumidores pueden ver sus transacciones procesadas en tan solo 10 minutos, 5 básicamente el tiempo que lleva agregar un bloque a blockchain, independientemente de la hora o el día de la semana. Con blockchain, los bancos también tienen la oportunidad de intercambiar fondos entre instituciones de manera más rápida y segura. En el negocio de negociación de acciones, por ejemplo, el proceso de liquidación y compensación puede demorar hasta tres días (o más, si los bancos operan internacionalmente), lo que significa que el dinero y las acciones se congelan durante ese tiempo.

Dado el tamaño de las sumas involucradas, incluso los pocos días en que el dinero está en tránsito pueden acarrear costos y riesgos significativos para los bancos. El banco europeo Santander y sus socios de investigación estiman los ahorros potenciales en $ 15 mil millones a $ 20 mil millones al año.7 Capgemini, una consultora francesa, estima que los consumidores podrían ahorrar hasta $ 16 mil millones en tarifas bancarias y de seguros cada año a través de aplicaciones basadas en blockchain.

Uso en criptomonedas

Blockchain forma la base de las criptomonedas como Bitcoin. Como exploramos anteriormente, las monedas como el dólar estadounidense están reguladas y verificadas por una autoridad central, generalmente un banco o un gobierno. Bajo el sistema de autoridad central, los datos y la moneda de un usuario están técnicamente al capricho de su banco o gobierno. Si el banco de un usuario colapsa o si vive en un país con un gobierno inestable, el valor de su moneda puede estar en riesgo. Estas son las preocupaciones de las que nació Bitcoin.

Al extender sus operaciones a través de una red de computadoras, blockchain permite que Bitcoin y otras criptomonedas operen sin la necesidad de una autoridad central. Esto no solo reduce el riesgo, sino que también elimina muchas de las tarifas de procesamiento y transacción. También les brinda a quienes se encuentran en países con monedas inestables una moneda más estable con más aplicaciones y una red más amplia de personas e instituciones con las que pueden hacer negocios, tanto a nivel nacional como internacional (al menos, este es el objetivo).

Usos sanitarios

Los proveedores de atención médica pueden aprovechar blockchain para almacenar de forma segura los registros médicos de sus pacientes. Cuando se genera y firma un registro médico, se puede escribir en la cadena de bloques, lo que proporciona a los pacientes la prueba y la confianza de que el registro no se puede cambiar. Estos registros de salud personales podrían codificarse y almacenarse en la cadena de bloques con una clave privada, de modo que solo ciertas personas puedan acceder a ellos, lo que garantiza la privacidad.

Uso de registros de propiedad

Si alguna vez ha pasado tiempo en la Oficina del Registrador local, sabrá que el proceso de registrar los derechos de propiedad es a la vez engorroso e ineficaz. Hoy, se debe entregar una escritura física a un empleado del gobierno en la oficina de registro local, donde se ingresa manualmente en la base de datos central del condado y en el índice público. En el caso de una disputa de propiedad, las reclamaciones sobre la propiedad deben conciliarse con el índice público.
Este proceso no solo es costoso y requiere mucho tiempo, sino que también está plagado de errores humanos, donde cada inexactitud hace que el seguimiento de la propiedad de la propiedad sea menos eficiente. Blockchain tiene el potencial de eliminar la necesidad de escanear documentos y rastrear archivos físicos en una oficina de grabación local. Si la propiedad de la propiedad se almacena y verifica en la cadena de bloques, los propietarios pueden confiar en que su escritura es precisa y permanente.
Uso en contratos inteligentes
Un contrato inteligente es un código de computadora que puede integrarse en la cadena de bloques para facilitar, verificar o negociar un acuerdo contractual. Los contratos inteligentes operan bajo un conjunto de condiciones que los usuarios aceptan. Cuando se cumplen esas condiciones, los términos del acuerdo se llevan a cabo automáticamente.

Digamos, por ejemplo, que te alquilo mi apartamento mediante un contrato inteligente. Acepto darte el código de la puerta del apartamento tan pronto como me pagues tu depósito de seguridad. Ambos enviaríamos nuestra parte del trato al contrato inteligente, que conservaría e intercambiaría automáticamente el código de mi puerta por su depósito de seguridad en la fecha del alquiler. Si no proporciono el código de la puerta antes de la fecha de alquiler, el contrato inteligente reembolsa su depósito de seguridad. Esto elimina las tarifas que normalmente acompañan al uso de un notario o un mediador externo.

Uso de la cadena de suministro

Los proveedores pueden usar blockchain para registrar el origen de los materiales que han comprado. Esto permitiría a las empresas verificar la autenticidad de sus productos, junto con etiquetas de salud y ética como "Orgánico", "Local" y "Comercio justo".
Como informó Forbes, la industria alimentaria se está moviendo hacia el uso de blockchain para rastrear cada vez más el camino y la seguridad de los alimentos a lo largo del viaje de la granja al usuario.

Usos en la votación

Votar con blockchain tiene el potencial de eliminar el fraude electoral y aumentar la participación de los votantes, como se probó en las elecciones de mitad de período de noviembre de 2018 en West Virginia. Cada voto se almacenaría como un bloque en blockchain, lo que los haría casi imposibles de manipular. El protocolo blockchain también mantendría la transparencia en el proceso electoral, reduciendo el personal necesario para llevar a cabo una elección y brindando a los funcionarios resultados instantáneos.

VENTAJAS Y DESVENTAJAS DE BLOCKCHAIN

A pesar de su complejidad, el potencial de blockchain como una forma descentralizada de mantenimiento de registros es casi ilimitado. Desde una mayor privacidad del usuario y una mayor seguridad hasta tarifas de procesamiento más bajas y menos errores, la tecnología blockchain puede ver aplicaciones más allá de las descritas anteriormente.

Pros

- Mayor precisión al eliminar la participación humana en la verificación
- Reducciones de costos al eliminar la verificación

de terceros
- La descentralización dificulta la manipulación
- Las transacciones son seguras, privadas y eficien-tes
- Tecnología transparente Contras
- Costo tecnológico significativo asociado con la

minería de bitcoins
- Transacciones bajas por segundo
- Historial de uso en actividades ilícitas
- Susceptibilidad a ser pirateado
- Estos son los puntos de venta de blockchain para

negocios en el mercado hoy con más detalle. Precisión de la cadena

Las transacciones en la red blockchain son aprobadas por una red de miles o millones de computadoras. Esto elimina casi toda la participación humana en el proceso de verificación, lo que resulta en menos errores humanos y un registro de información más preciso. Incluso si una computadora en la red cometiera un error computacional, el error solo se produciría en una copia de la cadena de bloques. Para que ese error se extienda al resto de la cadena de bloques, debería ser realizado por al menos el 51% de las computadoras de la red, algo casi imposible.

Reducciones de costos

Por lo general, los consumidores pagan a un banco para verificar una transacción, a un notario para firmar un documento o a un ministro para celebrar un matrimonio. Blockchain elimina la necesidad de verificación de terceros y, con ello, sus costos asociados. Los dueños de negocios incurren en una pequeña tarifa cada vez que aceptan pagos con tarjetas de crédito, por ejemplo, porque los bancos tienen que procesar esas transacciones. Bitcoin, por otro lado, no tiene una autoridad central y prácticamente no tiene tarifas de transacción.
Descentralización

Blockchain no almacena ninguna de su información en una ubicación central. En cambio, la cadena de bloques se copia y se distribuye a través de una red de computadoras. Cada vez que se agrega un nuevo bloque a la cadena de bloques, cada computadora en la red actualiza su cadena de bloques para reflejar el cambio. Al difundir esa información a través de una red, en lugar de almacenarla en una base de datos central, blockchain se vuelve más difícil de manipular. Si una copia de la cadena de bloques cayera en manos de un pirata informático, solo una copia de la información, en lugar de toda la red, se vería comprometida.

Transacciones eficientes

Las transacciones realizadas a través de una autoridad central pueden tardar unos días en liquidarse. Si intenta depositar un cheque el viernes por la noche, por ejemplo, es posible que no vea fondos en su cuenta hasta el lunes por la mañana. Mientras que las instituciones financieras operan durante el horario comercial, cinco días a la semana, blockchain funciona las 24 horas del día, los siete días de la semana. Las transacciones se pueden completar en unos diez minutos y se pueden considerar seguras después de unas pocas horas. Esto es particularmente útil para las transacciones transfronterizas, que generalmente toman mucho más tiempo debido a problemas de zona horaria y al hecho de que todas las partes deben confirmar el procesamiento de pagos.

Transacciones privadas

Muchas redes blockchain operan como bases de datos públicas, lo que significa que cualquier persona con una conexión a Internet puede ver una lista

del historial de transacciones de la red. Aunque los usuarios pueden acceder a detalles sobre transacciones, no pueden acceder a información de identificación sobre los usuarios que realizan esas transacciones. Es un error común pensar que las redes blockchain como bitcoin son anónimas, cuando en realidad solo son confidenciales.

Es decir, cuando un usuario realiza transacciones públicas, su código único llamado clave pública se registra en la cadena de bloques, en lugar de su información personal. Aunque la identidad de una persona todavía está vinculada a su dirección de blockchain, esto evita que los piratas informáticos obtengan la información personal de un usuario, como puede ocurrir cuando un banco es pirateado.

Transacciones seguras

Una vez que se registra una transacción, la red blockchain debe verificar su autenticidad. Miles o incluso millones de computadoras en la cadena de bloques se apresuran a confirmar que los detalles de la compra son correctos. Una vez que una computadora ha validado la transacción, se agrega a la cadena de bloques en forma de bloque. Cada bloque de la cadena de bloques contiene su propio hash único, junto con el hash exclusivo del bloque anterior. Cuando la información de un bloque se edita de alguna manera,
El código hash del bloque cambia; sin embargo, el código hash del bloque posterior no lo haría. Esta discrepancia hace que sea extremadamente difícil cambiar la información en la cadena de bloques sin previo aviso.

Transparencia

Aunque la información personal en la cadena de bloques se mantiene privada, la tecnología en sí es casi siempre de código abierto. Eso significa que los usuarios de la red blockchain pueden modificar el código como mejor les parezca, siempre que tengan la mayoría de la potencia computacional de la red que los respalde. Mantener los datos en el código abierto de la cadena de bloques también hace que la manipulación de los datos sea mucho más difícil. Con millones de computadoras en la red blockchain en un momento dado, por ejemplo, es poco probable que alguien pueda hacer un cambio sin ser notado.

DESVENTAJAS DE BLOCKCHAIN

Si bien hay ventajas significativas para la cadena de bloques, también existen desafíos importantes para su adopción. Los obstáculos para la aplicación de la tecnología blockchain en la actualidad no son solo técnicos. Los verdaderos desafíos son políticos y regulatorios, en su mayor parte, por no hablar de las miles de horas (léase: dinero) de diseño de software personalizado y programación de back-end necesarias para integrar blockchain a las redes comerciales actuales. Estos son algunos de los desafíos que se interponen en el camino de la adopción generalizada de blockchain.

Costo de tecnología

Aunque blockchain puede ahorrar dinero a los usuarios en tarifas de transacción, la tecnología está lejos de ser gratuita. El sistema de “prueba de trabajo” que usa bitcoin para validar transacciones, por ejemplo, consume grandes cantidades de poder computacional. En el mundo real, la energía de los millones de computadoras en la red bitcoin es cercana a la que consume Dinamarca anualmente. Suponiendo costos de electricidad de $ 0.03 ~ $ 0.05 por kilovatio hora, los costos de minería sin incluir los gastos de hardware son de aproximadamente $ 5,000 ~ $ 7,000 por moneda.

A pesar de los costos de extraer bitcoins, los usuarios continúan aumentando sus facturas de electricidad para validar las transacciones en la cadena de bloques. Eso es porque cuando los mineros agregan un bloque a la cadena de bloques de bitcoin, son recompensados con suficientes bitcoins para que su tiempo y energía valgan la pena. Sin embargo, cuando se trata de cadenas de bloques que no utilizan criptomonedas, los mineros deberán recibir un pago o incentivarlos de alguna otra manera para validar las transacciones.

Ineficiencia de velocidad

Bitcoin es un caso de estudio perfecto para las posibles ineficiencias de blockchain. El sistema de "prueba de trabajo" de Bitcoin tarda unos diez minutos en agregar un nuevo bloque a la cadena de bloques. A ese ritmo, se estima que la red blockchain solo puede administrar alrededor de siete transacciones por segundo (TPS) .11 Aunque otras criptomonedas como Ethereum funcionan mejor que bitcoin, todavía están limitadas por blockchain. Marca heredada Visa, por contexto , puede procesar 24.000 TPS.

Actividad ilegal

Si bien la confidencialidad en la red blockchain protege a los usuarios de los ataques y preserva la privacidad, también permite el comercio y la actividad ilegal en la red blockchain. El ejemplo más citado del uso de blockchain para transacciones ilícitas es probablemente Silk Road, un mercado en línea de la "web oscura" que opera desde febrero de 2011 hasta octubre de 2013, cuando fue cerrado por el FBI.
El sitio web permitía a los usuarios navegar por el sitio web sin ser rastreados y realizar compras ilegales en bitcoins. Las regulaciones actuales de los EE. UU. Requieren que los proveedores de servicios financieros obtengan información sobre sus clientes cuando abren una cuenta, verifican la identidad de cada cliente y confirman que los clientes lo hacen. no aparecer en ninguna lista de organizaciones terroristas conocidas o sospechosas.

Preocupaciones del banco central

Varios bancos centrales, incluida la Reserva Federal, el Banco de Canadá17 y el Banco de Inglaterra, 18 han iniciado investigaciones sobre monedas digitales. Un documento de junio de 2020 del Banco de la Reserva Federal de Filadelfia dijo que la creación de una moneda digital del banco central (CBDC) pondría a la Fed en competencia directa con los bancos privados. "Además de su papel potencial en la eliminación de efectivo físico, una CBDC permitirá al banco central participar en una intermediación a gran escala compitiendo con instituciones financieras privadas por depósitos (y, probablemente, participando en algunos préstamos de esos depósitos)", el dijo el papel. "En otras palabras, una CBDC equivale a brindar a los consumidores la posibilidad de tener una cuenta bancaria directamente en el banco central".

Hackear susceptibilidad

Las criptomonedas más nuevas y las redes blockchain son susceptibles a ataques del 51%. Estos ataques son extremadamente difíciles de ejecutar debido a la potencia computacional requerida para obtener el control mayoritario de una red blockchain, pero el investigador de ciencias de la computación de la NYU, Joseph Bonneau, dijo que eso podría cambiar. En 2017, Bonneau presentó un documento en el que se estimaba que era probable que aumentaran los ataques del 51%, ya que los piratas informáticos ahora pueden simplemente alquilar energía computacional, en lugar de comprar todo el equipo.

¿Y DESPUÉS DEL BLOCKCHAIN?

Propuesto por primera vez como un proyecto de investigación en 1991,3 blockchain se está asentando cómodamente en sus últimos veinte años. Como la mayoría de los millennials de su época, blockchain ha sido objeto de un gran escrutinio público durante las últimas dos décadas, y las empresas de todo el mundo especulan sobre lo que la tecnología es capaz de hacer y hacia dónde se dirige en los próximos años.

Con muchas aplicaciones prácticas para la tecnología que ya se están implementando y explorando, blockchain finalmente se está haciendo un nombre a los veintisiete años, en gran parte debido a bitcoin y criptomonedas. Como palabra de moda en la lengua de todos los inversores de la nación, blockchain hace que las operaciones comerciales y gubernamentales sean más precisas, eficientes y seguras.
Mientras nos preparamos para adentrarnos en la tercera década de blockchain, ya no se trata de "si" las empresas heredadas captarán la tecnología, es una cuestión de "cuándo".

Fuente: https://www.investopedia.com/terms/b/blockchain.asp


ACCELERALIA
acceleration platform