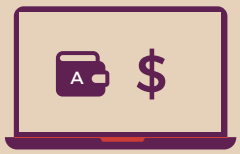
kipus Communications & Media Lab

Blockchain y algunos conceptos clave asociados

Cómo funciona blockchain

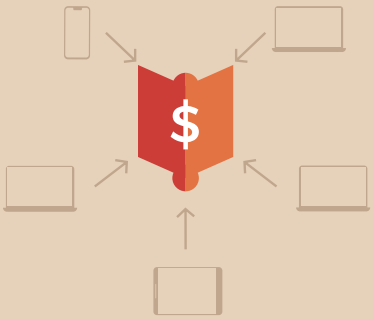
1. A quiere enviar dinero a B



2. La transacción se representa en la red como un “bloque”

3. El bloque se transmite a todas las partes de la red

4. Los que están en la red aprueban que la transacción es válida



5. El bloque entonces puede añadirse a la cadena, lo que proporciona un registro indeleble y transparente sobre las transacciones

6. El dinero se mueve de A a B

VIDEO
Blockchain y su aplicación en el ámbito financiero

MINADO

El minado de bloques consiste en la realización de una serie de complejos cálculos que requieren tiempo y (cada vez más) electricidad, pero cuando mediante este proceso esos bloques quedan registrados, lo hacen de forma permanente en esa cadena de bloques, y no pueden ser modificados sin que se alteren todos los bloques que están enlazados con él, una operación que además necesitaría que la mayoría de los nodos la validen.

HASH

Ese libro de cuentas no solo está distribuido y es seguro: los bloques enlazados (de ahí lo de cadena de bloques) cuentan con un puntero hash (un algoritmo) que enlaza al bloque anterior, además de una marca de tiempo y los datos de la transacción, y esa información es pública. ¿Qué significa eso? Que la cadena de bloques, aunque protege la privacidad de sus usuarios, sí que permite controlar la trazabilidad de esas transacciones.

O lo que es lo mismo: permite saber todo el camino que han seguido los 1000 dólares (o cualquier otro tipo de activo, mercancía, etc.) de la wallet que pertenece a alguien (en este caso, la primera persona, aunque su identidad no se conoce por el resto de usuarios) antes de llegar a la cartera de la persona receptora de los 1000 dólares.

Esto, cualidad propia del diseño de la cadena de bloques, tiene ventajas claras, y por ejemplo confirma que cada unidad de valor (por ejemplo, un bitcoin) solo se ha transferido una única vez, lo que evita el tradicional problema con el doble gasto de monedas digitales o con el dinero falso, que reduce la confianza de los usuarios en esa moneda y también en la propia circulación de la misma.

WALLET

Una wallet es un software que almacena tus claves públicas y privadas (siempre van juntas) y te permite enviar y recibir criptomonedas a través de la Blockchain, almacenar las que quieras y controlar siempre que quieras tu saldo.

SMART CONTRACT

Un contrato no es más que un acuerdo entre dos o más partes, un documento donde se define lo que se puede hacer, cómo se puede hacer, qué pasa si algo no se hace. O sea, unas reglas de juego que permiten a todas las partes que lo aceptan entender en qué va a consistir la interacción que van a realizar.

Hasta ahora los contratos han sido documentos verbales o caros documentos escritos. Estos documentos están sujetos a las leyes y jurisdicciones territoriales, y en ocasiones requieren de notarios o escribanos. Es decir, más costes, tiempo y terceros que intervienen en el proceso. Debido a ello, no son accesibles para cualquier persona. Y esto no es lo peor: los contenidos de los contratos pueden estar sujetos a la interpretación.

En cambio un contrato inteligente es capaz de ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática, sin intermediarios ni mediadores. Evitan el lastre de la interpretación al no ser verbal o escrito en los lenguajes que hablamos. Los smart contracts se tratan de “scripts” (códigos informáticos) escritos con lenguajes de programación. Esto quiere decir que los términos del contrato son puras sentencias y comandos en el código que lo forma.

Además, un smart contract puede ser creado y llamado por personas físicas y/o jurídicas, pero también por máquinas u otros programas que funcionan de manera autónoma. Un smart contract tiene validez sin depender de autoridades. Esto se debe a su naturaleza: es un código visible por todos y que no se puede cambiar al existir en bloques dentro de una blockchain. Esto le confiere un carácter descentralizado, inmutable y transparente.

TOKEN

El término token estuvo vinculado desde sus orígenes a los primeros sistemas financieros. El token estuvo vinculado desde aquel momento a una especie de ficha o pseudomoneda que poseía la función de sustituir la moneda real en una relación financiera específica manteniendo la capacidad operativa. El ejemplo clásico que podemos citar es el de las fichas de casino, pero se

puede tokenizar cualquier activo: barriles de petróleo, donaciones, cereales, ganado, etc., y, por supuesto, criptomonedas.

ACTIVO DIGITAL

Cualquier recurso que existe de forma digitalizada y que alguien puede poseer o que representa contenido que alguien también puede poseer y, por lo tanto, tiene un derecho para su uso. Al tratarse como una propiedad, puede venderse, comprarse o licenciarse.

ALGORITMO

Conjunto de instrucciones o reglas previamente escritas, bien definidas, ordenadas y finitas que permite llevar a cabo una actividad mediante pasos sucesivos que no generan dudas a quien deba hacer dicha actividad. Dados un estado inicial y una entrada, se llega a un estado final y se obtiene una solución.

BASE DE DATOS DISTRIBUIDA

Se trata de un conjunto de información mantenida por diversos participantes de un nodo en una red. No existe un administrador central ni un almacenamiento de datos centralizado. Requiere una red punto a punto o entre pares (peer to peer o P2P), así como consensos para garantizar la replicación a través de los nodos.

BLOCKCHAIN PRIVADA

Aquella en la que el proceso de consulta, validación y participación están limitados a unos nodos específicos. Tanto los accesos a los datos de la cadena de bloques como el envío de esos datos para ser incluidos, están limitados a una lista predefinida de nodos. Ejemplo: una cadena construida sobre la red de Ethereum exclusivamente entre dos bancos.

BLOCKCHAIN PÚBLICA

Aquella en la que no hay restricciones ni para leer los datos de la cadena de bloques ni para validar transacciones para que sean incluidas en la cadena de bloques. En ellas es fácil entrar y salir, son transparentes; están construidas para operar en un entorno sin necesidad de confianza. Ejemplo: Blockchain de Bitcoin.

CRIPTOGRAFÍA

Técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

CÓDIGO ABIERTO (OPEN SOURCE)

Modelo de desarrollo de software basado en la colaboración abierta. Permite modificar el código fuente del programa sin restricciones de licencia. Los programadores pueden leer, modificar y redistribuir el código fuente de un programa, de forma que éste evoluciona, se desarrolla y mejora. Los usuarios los adaptan a sus necesidades; corrigen sus errores con un tiempo de espera menor a la aplicada en el desarrollo de software convencional o cerrado, dando como resultado la producción de un mejor software.

POW

PoW o prueba de trabajo > Se trata de un protocolo de consenso distribuido en el que la cadena con más apoyo es la cadena con más trabajo detrás. Es un hash con unos requisitos determinados para que sea difícil encontrar por el minero. El minero obtiene tokens o criptomonedas de esa blockchain como recompensa.

POS

PoS o prueba de participación > Protocolo de consenso distribuido en el que la probabilidad de que un staker encuentre un bloque de transacciones y reciba el incentivo correspondiente es

directamente proporcional a la cantidad de monedas que tiene acumuladas. La cadena con más apoyo es la cadena con más colateral o stake destinado. El staker necesita comprar tokens para validar bloques.

ETHEREUM

Plataforma open source, descentralizada y basada en el modelo Blockchain que permite la creación de contratos inteligentes. Utiliza un sistema de consenso de tipo PoW. Habilita la ejecución de contratos inteligentes sobre su red, gracias al aporte de los mineros, que son recompensados con Ethers, el token que utiliza esta red.

GAS

Precio interno para ejecutar una transacción o contrato en Ethereum. Se utiliza para desacoplar la unidad Ether (ETH) y su valor de mercado de la unidad para medir el uso computacional (GAS).

MONEDA FIAT

Dinero de curso legal. Únicamente los bancos centrales tienen el poder de emitir dinero fiar (dólar, euro, sol, etc.).

LA CADENA DE BLOQUES MÁS ALLÁ DE LA ECONOMÍA

Aunque la cadena de bloques está íntimamente relacionada con las nuevas criptodivisas o criptomonedas, es lógico preguntarse si este sistema sería válido para otro tipo de transacciones, y la respuesta es un rotundo sí.

De hecho, eso es lo que está intentando lograr desde sus inicios la plataforma Ethereum, que tiene su propia cadena de bloques (podéis echarle un vistazo en sitios como Etherscan.io) y su propia moneda, llamada Ether. A diferencia de bitcoin, las transacciones aquí son los contratos inteligentes, que pueden ser más o menos complejos y que permiten definir todo tipo de transacciones.

LAS OPORTUNIDADES

A continuación, enunciamos algunas aplicaciones concretas de la tecnología Blockchain al sistema financiero. Para eso, seguiremos los últimos informes sobre inclusión financiera del Banco Interamericano de Desarrollo y del Banco Mundial junto con el conocimiento brindado por Koibanx.

AHORROS Y CUENTAS TRANSACCIONALES:

El mayor desarrollo sobre tecnología Blockchain siguen siendo las criptomonedas. Por definición, estas permiten la reserva de valor, entre otros beneficios. Es decir, ahorro. Por ejemplo, al menos teóricamente, cualquiera que utilice Bitcoin tiene el equivalente a una cuenta bancaria en línea en forma de billetera virtual basada en Blockchain . Obtener esta billetera es gratis y está disponible para cualquier persona con conocimientos en la temática y acceso a Internet. Incluso, algunos proveedores de billeteras ya están trabajando en soluciones por SMS. No se requiere identificación legal, solo una dirección de correo electrónico o un número de teléfono, y no hay cargos de mantenimiento ni requisitos de saldo mínimo (en algunos exchanges se puede acceder a una fracción de BTC a partir de los cien pesos argentinos). Así, tal como proponía Nakamoto —creador del Bitcoin—, las barreras de acceso desde el lado de la oferta quedarían derribadas.

FINANCIAMIENTO Y EVALUACIÓN CREDITICIA ALTERNATIVA:

El empleo de Blockchain presenta beneficios para automatizar la suscripción y el desembolso de fondos, lo que posibilita reducir el tiempo de emisión de préstamos y el riesgo operativo. Además, almacenar detalles financieros puede facilitar la aprobación en tiempo real de solicitudes financieras, crear nuevas estructuras de financiación, achicar el riesgo de contraparte, permitir una liquidación más rápida de los préstamos y brindar ventajas para el financiamiento entre pares.

PAGOS Y REMESAS INTERNACIONALES:

El dinero o banca móvil y los pagos electrónicos tradicionales reducen de manera drástica los costos de transferencia al evitar el gasto fijo de las sucursales. A su vez, traen beneficios obvios de conveniencia y reducen los costos de transporte, especialmente en poblaciones aledañas (la gente ya no tiene que ir a la ciudad para manejar sus asuntos financieros). Sin embargo, en estos términos, los desarrollos en Blockchain no parecieran tener demasiadas ventajas por sobre los pagos electrónicos tradicionales para la demanda. Ahora bien, sin duda alguna, cuando hablamos de pagos internacionales o remesas, la situación es muy diferente. Los altos costos de los intermediarios financieros en estos casos significan que el potencial disruptivo de la tecnología Blockchain y las criptomonedas sea mucho mayor que en los pagos locales.

Esto se explica porque incluso los servicios de remesas que funcionan a través de Internet o que utilizan dinero móvil recurren al sistema bancario (normalmente bancos corresponsales) para liquidar las transacciones transfronterizas. Para ello necesitan varios días para liquidar las transacciones. Aun cuando a un precio mayor ofrezcan servicios de entrega casi inmediata, es la institución intermediaria la que adelanta el pago a la espera de recibir la transferencia una vez aprobada. Esto incrementa sus costos de capital. Con el uso de Blockchain directamente se omite este paso. Así se reducen los costos de capital y las barreras de entrada para las nuevas empresas, lo que intensifica la competencia. Por su diseño, las transacciones con Blockchain no tienen fronteras: la misma tarifa mínima (unos pocos centavos de dólar) se cobra independientemente del lugar donde residan los dos lados de una operación.

De esta forma, los ciudadanos que carecen de un acceso adecuado al sistema financiero pueden obtener una mayor independencia y mejores oportunidades de bienestar mediante la creación de una identidad digital en Blockchain.

DONACIONES Y FINANCIAMIENTO AL DESARROLLO:

Con esta tecnología, las donaciones entre pares (P2P) pueden realizarse sin la ayuda de organizaciones intermediarias como ONGs, organizaciones comunitarias o cualquier otro actor en la cadena de ayuda, así como de instituciones financieras. Esto asegura que una mayor proporción de donaciones y de préstamos llegue a los beneficiarios, y que se puedan incorporar contratos inteligentes para asegurar que el dinero se utilice según lo previsto.

COMERCIO, EXPORTACIONES Y LOGÍSTICA

Las nuevas tecnologías son una puerta hacia la disrupción de los servicios logísticos y el comercio tal como los conocemos. Desde la robótica y la automatización de procesos y transporte hasta Internet de las Cosas o la impresión 3D, todas estas herramientas están generando nuevos paradigmas. Y Blockchain está haciendo lo suyo para el comercio en general.

La Organización Mundial del Comercio, por ejemplo, plantea tres grandes dimensiones a través de las cuales esta tecnología promete revolucionar el comercio internacional: a) aumento de la confianza y la transparencia en las cadenas de valor, b) reducción de los costos comerciales y c) oportunidades para las PYMES y pequeños productores de los países en desarrollo.

LINK
Glosario/Diccionaro Blockchain

LINK
Diccionario básico de ‘blockchain’: diez términos que debes conocer