BlockChain: La tecnología que descentraliza al mundo.

José Guggiari
Asunción, Paraguay
jpgb010@gmail.com

Resumen

Este paper es un informe sobre el estado de la tecnología Blockchain y las nuevas plataformas que surgieron a partir de ella. Se concentra en las aplicaciones mas allá del bitcoin u otras monedas criptograficas y en el aporte a la sociedad que puede brindar un mundo descentralizado.

KEYWORDS

blockchain, criptografía, bitcoin, criptomonedas, ethereum, economía, contratos inteligentes,agentes inteligentes, peer to peer, Wei, gas.

1. INTRODUCTION

Casi todos los servicios que utilizamos hoy en día requieren que el usuario se conecte a un servidor para acceder a una aplicación o servicio en concreto. Esta forma de acceder a contenido, que ah funcionado desde la introducción de la internet, es centralizada con todos los problemas que esto acarrea, como la caída de servicios, censura por parte de gobiernos y la confianza en los proveedores de estos servicios es un factor determinante. Blockchain llega para cambiar esto. Nacido en Octubre del 2008, fue creado por Satoshi Nakamoto, un seudónimo o alias de una persona o varias, para crear la primera criptomoneda, Bitcoin, que resolvía varios problemas de los anteriores intentos de monedas electrónicas, como el doble gasto, la reversibilidad de las transacciones y la necesidad de la confianza para realizar las transacciones.Bitcoin supuso una revolución en el ámbito financiero. Ya no es necesario contar con una cuenta bancaria y pagar enormes comisiones o impuestos para transferir dinero a cualquier parte del mundo en poco tiempo y la moneda no estaba atada a los caprichos de un banco central que pudiese devaluar la moneda. Pero la tecnología Blockchain puede ofrecer mucho mas que una moneda digital.

Creado por Satoshi Nakamoto, un seudónimo o alias de una persona o varias, para crear la primera criptomoneda, Bitcoin.

Tomando el mismo concepto de redes peer-to-peer y adaptando el código de Bitcoin, nace en el 2010 el primer uso alternativo: Namecoin, una base de datos de registros de nombres descentralizada, básicamente un servidor DNS corriendo sobre BlockChain, logrando independizar los dominios registrados en su red de la ICANN y descentralizando el registro de dominios.

Llevando el protocolo al límite, por lo menos por ahora, nació Ethereum, una plataforma de aplicaciones y contratos inteligentes montada sobre una red Blockchain propia. Ethereum, aún en su primera versión abierta al público, permite a sus usuarios alojar aplicaciones o servicios enteros en la red descentralizada, donde para poder publicar es necesario pagar una cantidad determinada de Ether, la moneda de Ethereum, y luego ya podemos almacenar nuestras aplicaciones, datos, contratos inteligentes o cualquier cosa que se nos ocurra. Es básicamente la descentralización total del internet como conocemos ahora.

2. COMO FUNCIONA BLOCKCHAIN

2.1. Las transacciones

Se define una moneda electrónica como una cadena de firmas digitales. Cada dueño transfiere esta moneda al siguiente dueño firmando un hash de la transacción previa con la llave pública del siguiente dueño y se agregan estos al final de la moneda. El receptor de la moneda puede verificar la firma para corroborar la cadena de propiedad.

El problema que surge a partir de esto es que el receptor no puede verificar que el dueño anterior no gaste dos veces la misma moneda. La única forma de prevenir esto es conociendo todas las transacciones realizadas. Para realizar esto, se debe anunciar públicamente todas las transacciones y se necesita que todas las partes estén de acuerdo con un solo historial del orden en que las transacciones fueron realizadas.

2.2. Servidor TimeStamp

BlockChain propone un servidor Timestamp. El servidor timestamp distribuido toma el hash de un bloque de transacciones y publica el hash en la red. Cada timestamp incluye el anterior, creando una cadena de bloques. Cuando se crea un nuevo bloque, que es verificado por los usuarios de la red y una vez verificado, oficialmente se convierte en parte de la cadena de bloques. Este proceso de verificación es hecho en una prueba de trabajo (proof of work) por mineros.

2.3. La prueba de trabajo

Un bloque se verifica cuando el nonce, un numero aleatorio que es utilizado una única vez, se encontró que, pasado por una función hash, proporciona un resultado menor que el valor objetivo. Una vez que el esfuerzo computacional satisface la prueba de trabajo, no se puede cambiar sin hacer de nuevo todo el trabajo, y, como los bloques están encadenados juntos, se deben calcular todos los bloques después de él también. Las pruebas de trabajo son esencialmente un sistema de una CPU, un voto. La decisión de la mayoría esta representada por la cadena mas larga, que tiene el mayor esfuerzo de pruebas de trabajo invertido. Si la mayor cantidad de poder computacional esta controlada por nodos honestos, la cadena honesta va a crecer más rápido que cualquier otra cadena en competencia. Para modificar un bloque pasado, para intentar robar bitcoins, un atacante debe rehacer todas las pruebas de trabajo y todos los bloques después de el y luego alcanzar y sobrepasar el trabajo de los nodos honestos. Esta posibilidad disminuye exponencialmente a medida que la cadena honesta crece. En la red Bitcoin, cada 2.016 bloques, la dificultad cambia. Si se crea un conjunto de bloques con demasiada rapidez, la dificultad aumenta, mientras que si se tarda demasiado tiempo para resolver un grupo de bloques, la dificultad disminuye. El marco de tiempo de destino es de dos semanas. La dificultad y los limites de tiempo van variando entre red y red.

2.4. Minería

1. Las nuevas transacciones se transmiten a todos los nodos

2. Cada nodo de la minería recoge nuevas transacciones en un bloque.

3. Cada nodo minero trabaja en la búsqueda de una prueba de trabajo para su bloque.

4. Cuando un nodo de la minería encuentra una prueba de trabajo, este transmite el bloque a todos los nodos.

5. Los demás nodos acepta el bloque sólo si todas las transacciones son válidas y no se hayan gastado.

6. Los nodos expresan su aceptación del bloque trabajando en la creación del próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash anterior.

3. CONTRATOS INTELIGENTES Y AGENTES AUTÓNOMOS

Los contratos inteligentes son contratos que no requieren la interpretación o la intervención humana para llevarse a cabo. La ejecución de estos contratos se realiza de forma automática al ejecutar un programa de ordenador. Los contratos inteligentes son contratos cuyo cumplimiento está basado en propiedades matemáticas (criptografía), a diferencia de los contratos legales. La transferencia de valor digital mediante un sistema que no requiere confianza abre la puerta a nuevas aplicaciones que pueden hacer uso de los contratos inteligentes.

Una de estas aplicaciones son los agentes autónomos. Los agentes autónomos no deben confundirse con la inteligencia artificial. Los agentes autónomos son simplemente programas de ordenador sencillos, creados para una tarea específica. Un ejemplo es un programa que se ejecuta en la nube y que alquila espacio de almacenamiento y ofrece a sus clientes finales un servicio de almacenamiento de archivos.

Hasta ahora los programas de ordenador no podían contener el valor : un programa informático no podía abrir una cuenta bancaria a su nombre. Con la introducción de Bitcoin, los programas de ordenador pueden controlar sus propios fondos y firmar contratos con proveedores de servicios en la nube, por ejemplo para alquilar almacenamiento y potencia de cálculo.

Del mismo modo, este agente autónomo podría firmar contratos inteligentes con sus usuarios finales. El agente autónomo puede liquidar estos contratos inteligentes realizando los pagos al proveedor de la nube y recibiendo los pagos de sus usuarios finales en bitcoins u otras criptomonedas con su propia red BlockChain.[1]

4. ETHEREUM

Ethereum es un proyecto que intenta construir una tecnología generalizada, sobre donde se construyen todas las maquinas de estados de transacciones. Trata de proveer al desarrollador final un sistema de punto a punto completamente integrado para construir software en, hasta ahora, un inexplorado paradigma computacional: un framework computacional de mensajería de confianza.

El principal objetivo es proveer un medio que , ya sean por cuestiones geográficas o sociales, dos individuos consientes que necesiten hacer una transacción pero no tengan un medio confiable, lo puedan hacer sin la necesidad de necesariamente confiar en la otra persona o un tercero. A través de un sistema de cambios de estado con un lenguaje rico y no ambiguo, se pueden crear acuerdos que se cumplan autónomamente, mediante smart contracts.[6]

4.1. Funcionamiento de Ethereum

Ethereum, al igual que bitcoin, es una maquina de estado basada en transacciones. Se inicia con un estado general y se ejecutan incrementalmente las transacciones hasta transformarse en un estado final. En este estado final, es aceptado como la versión canónica del mundo de Ethereum. El estado puede incluir información como balance de una cuenta,

reputación, acuerdos, datos sobre el mundo físico; básicamente cualquier cosa que pueda ser representada por una computadora es admisible. Las transacciones se representan como un arco valido entre dos estados; la validación es un parte importante, existen muchos mas cambios a estados inválidos que válidos. Un cambio a un estado inválido podría reducir el balance de una cuenta sin un incremento proporcional en otras cuenta. Una transición de estado valida es aquella que se produce a través de una transacción.

Las transacciones se cotejan en bloques; luego estos son encadenados juntos usando un hash criptográfico como un medio de referencia. Los Bloques funcionan como un diario, registrando una serie de operaciones junto con el bloque anterior y un identificador para el estado final (aunque no guarda el estado final, sería demasiado grande). También marcan la serie de transacciones con incentivos para que los nodos sean minados. Este incentivo tiene lugar como una función de transición declaración, agregando valor a una cuenta designada.[2]

4.1.1. Valor

Con el fin de incentivar la computación dentro de la red, es necesario que haya un método acordado para transmitir valor. Para solucionar este problema, Ethereum tiene una moneda intrínseca, Ether, conocido también como ETH. La denominación más pequeña de Ether, es el Wei. Un éter se define como Wei. Existen otras sub denominaciones de Ether:

Multiplicador	Nombre
10^0	Wei
10^{12}	Szabo
10^{15}	Finney
10^{18}	Ether

4.1.2. La transacción

Una transacción es una sola instrucción criptográficamente firmada construida por un actor externo al alcance de Ethereum. Mientras se asume que el último actor externo será humano en naturaleza, herramientas de software serán utilizados en su construcción y diseminación . Hay dos tipos de transacciones: las que dan lugar a las llamadas de mensajes y las que dan lugar a la creación de nuevas cuentas con código asociado (conocida informalmente como çreación de contratos). Ambos tipos especifican un número de campos comunes:

- nonce: Escalar de valor igual al numero de transacciones enviadas por el emisor.
- gasPrice: Escalar de valor igual en Wei a ser pagado por unidad de gas por todo el costo computacional incurrido como resultado de la ejecución de esta transacción.
- gasLimit: Escalar de valor igual al máximo monto de gas que debe ser usado para ejecutar estación y no puede ser incrementada luego.
- to: Dirección de 160 bits del receptor de la llamada de mensaje, para la creación de una transacción de tipo contrato.
- value: Escalar de valor igual al numero de Wei a ser transferido al receptor de la llamada de mensaje, en el caso de la creación de un contrato, como una dotación a la cuenta creada.
- v,r,s: Valores correspondientes a la firma de la transacción, son usados para determinar el emisor de la transacción.

Los contratos creados por las transacciones contienen también:

- init: Un arreglo de tamaño indeterminado específico para el procedimiento de inicialización de la cuenta. Es ejecutado una sola vez y descartado luego de la creación de la cuenta.

En contraste, una llamada de mensaje contiene:

- data: Un arreglo de tamaño indeterminado que contiene los valores de entrada de un mensaje.

4.1.3. El bloque

El bloque en Etereum es la colección de piezas relevantes de información (conocida como la cabecera del bloque), junto con la información correspondiente a las operaciones comprendidas, y un conjunto de otras cabeceras de bloque que se sabe que tienen un padre igual al padre del bloque actual (tales bloques son conocidos como ommers2).

4.1.4. Recibo de la transacción

Con el fin de codificar información acerca de una transacción y para la cual resulta útil formar una prueba de conocimiento cero, o un índice y búsqueda, se codifica un recibo de cada transacción que contiene la información relativa a su ejecución. Cada recibo se coloca en un índice y la raíz se registra en la cabecera.

4.1.5. Gas y pagos.

Para evitar problemas de abuso de las red y para esquivar el inevitable cuestionamiento originado por la completitud de Turing, toda computación programable en Ethereum esta sujeto a tarifas. La tarifa calendarizada es especificada en unidades de Gas (agregar apéndice C del paper para las tarifas). Así, cualquier fragmento de programa tiene un costo universal en términos de gas. Cada transacción tiene un monto de gas específico a pagar llamado gasLimit, que representa el monto que es implícitamente comprado desde la cuenta del remitente. Este compra se realiza de acuerdo al gasPrice, también especificado en la transacción. Este es considerada invalida si el remitente no posee los fondos necesarios.

En general, el Ether usado para comprar gas que no es devuelto, se envía a la dirección del beneficiario, que esta bajo el control del minero. Las partes son libres de especificar un monto de gasPrice arbitrario, en contraste con los mineros que pueden ignorar las transacciones si así lo desean. Un costo elevado de gas en una transacción costaría mas en términos de Ether al remitente y enviaría un mayor valor al minero y tendría mas posibilidades de ser seleccionado

por los mineros. Estos, en general, elegirían anunciar el menor costo de gas para el cual estarían dispuestos a ejecutar transacciones y las partes en la transacción son libres de determinar estos precios. Como hay una distribución ponderada del mínimo precio de gas, los que realicen transacciones necesariamente tendrían que balancear el precio del gas y las probabilidades de que sus transacciones sean minadas en un tiempo razonable.

4.1.6. Ejecución de las transacciones

La ejecución de una transacción es la parte mas compleja de Ethereum: Define el estado de transición. Asume que cualquier transacción ejecutada ha pasado un control inicial de valor intrínseco. Estos incluyen:

1. Tienen un RLP bien formado, sin bytes adicionales.
2. La firma de transacción es valida.
3. El nonce es válido
4. El limite de gas no es menor al valor intrínseco.
5. El saldo de la cuenta del remitente contiene al menos el costo requerido para el pago adelantado.

4.1.7. Recompensas

La aplicación de recompensas a un bloque implica elevar el saldo de las cuentas de la dirección de los beneficiarios del bloque y cada ommer por un cierta cantidad.

La recompensa de un bloque se define en 5 Ether, la dirección del beneficiario recibe estos 5 Ether; para cada ommer, se aumenta nuevamente en un 1/32 de la recompensa del bloque y el beneficiario del ommer recibe una recompensa dependiendo del numero del bloque. Si la dirección del beneficiario y del ommer son las mismas, estas recompensas se suman.

4.2. Implementación de los contratos

Las aplicaciones de los smart contracts son incontables, desde aplicaciones puramente académicas hasta revoluciones sociales complejas como sistemas de votación descentralizados y extremadamente difíciles de corromper dada la complejidad de la tecnología blockchain y su fuerte base criptografica.

4.2.1. Feeds de datos

Un contrato de suministro de datos proporciona un único servicio: Da acceso a información desde el mundo externo a Ethereum. La precisión e invariabilidad de esta información en el tiempo no esta garantizada y depende de un contrato secundario, el contrato que utiliza este feed de datos, para determinar cuanta confianza puede ser depositada en una sola fuente de datos. El caso general consiste en un solo contrato dentro de Ethereum que, cuando se realiza una llamada de mensaje, responde con información relativa a un fenómeno externo. Un ejemplo podría ser la temperatura local de una ciudad. Esto se implanta a través de un contrato que devuelve este valor de algún punto conocido en el almacenamiento. Este punto debe mantenerse con la temperatura correcta y por lo tanto la segunda parte de este caso consiste en un servidor externo corriendo un nodo Ethereum que cuando descubre un nuevo bloque, crea una nueva transacción valida, envía el contrato actualizando el valor almacenado. El código de este contrato aceptaría tales actualizaciones solo de la identidad contenida en dicho servidor.

4.2.2. Coleccionables Digitales y el sistema actual de cupones de descuento y fidelización de clientes

La complejidad y la sofisticación de los consumidores, que disponen cada vez más fuentes de información para realizar compras inteligentes, genera un incremento de la competencia en el sector minorista que hace que las empresas les resulte cada vez más difícil captar nuevos clientes y mantenerlos en el tiempo. Por este motivo se crearon las ya muy conocidas tarjetas de fidelidad. Estas tarjetas proveen beneficios exclusivos para compradores fieles como descuentos o promociones especiales que agregan valor a una compra mas allá del precio real del producto que adquieren.

Tradicionalmente estas tarjetas poseen un formato físico y en los últimos años se popularizó la digitalización de estas tarjetas a través de sistemas in-house de las empresas o a través de proveedores externos como Apple Pay y Google Wallet.

Estas implementaciones tienen distintos problemas: Las tarjetas físicas se pierden y las digitales son costosas de mantener en sistemas propios, y las tercerizadas tienen un costo que en el tiempo se llevan una tajada importante del beneficio que podría recibir la empresa con su utilización.

Aquí es donde los contratos inteligentes podrían ayudar a solventar estos problemas.

Un sistema de cupones ejecutado a través de contratos inteligentes alojados en una red BlockChain, por ejemplo Ethereum, solventa estos problemas.

Los cupones, frecuentemente, son de uso único y personales. La red BlockChain junto a un contrato inteligente puede verificar la autenticidad de este cupón y marcarlo como ya utilizado, gastando una cantidad de Ether asociada al cupón, haciéndola inútil por una segunda vez o un numero predeterminado de usos. Solamente la persona dueña de la dirección puede gastarla firmando con su llave privada la transacción.

Los costos de mantener este sistema estaría ligado al precio del Ether, pero siempre se puede optar por asociar un cupón con una unidad menor como el Wei y así utilizar la menor cantidad de dinero para generar estos cupones.

Una empresa podría también adoptar un mercado interno de cupones, donde los usuarios intercambian cupones que les sobra por otras ofertas que son de su interés. [5]

4.2.3. Sistemas de votación

Muchas organizaciones, ya sean privadas o públicas, tienen sistemas muy pobres para realizar votaciones. Muchos de estos votos son tomados a viva voz, un proceso que no registra los votos. Si algún tipo de contabilidad es llevado a cabo, no siempre es registrado, y si lo es, no es perfecto. Un ejemplo concreto son las Cámaras de Senadores y Diputados de la República del Paraguay, donde las leyes son votadas a

viva voz, por turno, llamados uno a uno en un proceso lento, tedioso, presencial y arcaico.

Registrando estos votos en una red BlockChain, se obtiene un registro permanente de todos los votos en el tiempo, asociados a individuos con un sello de tiempo (timestamp) y un resultado.

No solo soluciona el problema de la organización de los votos, sino otros como la transparencia, haciendo accesible el resultado de una votación a todos los usuarios de la red, en tiempo real. La presencia de los votantes en una localización geográfica especifica para realizar el voto tampoco es necesario bajo este sistema, el único requerimiento es la llave privada del usuario.

4.2.4. Comercio internacional: El problema del transporte de bienes

El transporte de bienes en un mundo globalizado como el nuestro se enfrenta una problemática de tediosa resolución: Si algo falla en el transporte. £Quien tiene la culpa?.

Actualmente la solución a este problema se realiza a través un documento llamado Conocimiento de embarque.

El conocimiento de embarque es un documento que se utiliza en el marco de un contrato de transporte de las mercancías en un buque en línea regular. La finalidad de este documento es proteger al cargador y al consignatario de la carga frente al naviero y dar confianza a cada parte respecto al comportamiento de la otra. [8] Un caso particular ocurrió en España, donde una empresa debía entregar un peso exacto de una mercadería a otra empresa transportista. La transportista se negó a firmar el conocimiento de embarque alegando que el peso de la mercadería excedía lo acordado, y que el flete debía aumentar. La empresa alego que independientemente del peso, el contrato ya estaba firmado y la transportista debía enviar el cargamento y cobrar el mismo flete, independientemente del peso real de la carga. La transportista se considero unilateralmente legitimado a retener el cocimiento de embarque y no entregarlo hasta que ese mayor flete exigido unilateralmente fuera abonado.[7]

El problema se resolvió luego de un largo litigio en Londres, con incontables gastos de representación en abogados, superando la diferencia de precio en el flete exigido por la transportista. Aquí identificamos varios problemas:

1. La confianza es un factor determinante en los negocios, especialmente en el comercio internacional.

2. Los contratos tradicionales en el mundo real son papeles son valor si una de las partes rompe el contrato unilateralmente.

3. Los procesos de solución de conflictos son lentos y caros

Nuevamente, podríamos proponer a una red BlockChain con agentes inteligentes y contratos inteligentes para intentar solucionar esos problemas.

Ya que los contratos inteligentes programados por un tercero imparcial eliminan el factor confianza de la ecuación. El contrato se ejecuta una vez cumplida una condición impuesta en su código y no se puede revertir la transacción que ejecuto el contrato, lo cual impide el no cumplimiento del contrato de forma unilateral. También elimina parcialmente la necesidad de un proceso judicial largo y costoso al ejecutar cláusulas automáticamente.

En el caso de la transportista y la empresa, podría utilizarse la primera aplicación propuesta en este documento: Los feeds de datos.

Un nodo conectado a un conjunto de sensores en la carga a ser transportada puede informar del estado de la carga en tiempo real. Por ejemplo:

GPS: Una carga debe recorrer una ruta preestablecida por ambas partes hasta el destino, si esta se desvía de su curso, el agente inteligente ejecuta el contrato automáticamente, sin intermediarios ni rompimiento de contrato unilaterales.

Sensores térmicos y de CO2 combinados nos pueden indicar un principio de incendio y junto a análisis de video pueden determinar su causa y ejecutar un contrato con una entidad aseguradora.

Balanzas digitales nos pueden indicar el peso total de la carga, solucionado la problemática de nuestro ejemplo sin llegar a discusiones ni procesos judiciales. Ademas de ser un indicador de robo de mercadería, nuevamente ejecutando un contrato con una aseguradora.

5. LA ADOPCIÓN DE LA TECNOLOGÍA

La comunidad Bitcoin crece día a día. Basta solo con ver el nivel de mercado actual. Solamente la red Bitcoin tiene un valor de 53,981,353.21 dólares americanos al cambio de 245.3 dólares por bitcoin.

Inicialmente, como toda tecnología nueva y disruptora, BlockChain causo opiniones dispares y cautelosas, especialmente de gobiernos que no veían con buenos ojos una tecnología que permitiera intercambios seudo anónimos con monedas no atadas al control de los bancos centrales. Algunos países como Ecuador, Rusia, Tailandia, Vietnam y Bolivia llegaron extremos como prohibir completamente las operaciones en bitcoin.

Se podría intuir, no sin razón, que los bancos serían los primeros en intentar frenar esta tecnología que tiene el potencial de reducir la cuota de mercado de estos, pero, no sin sorprender a muchos, 9 de los mas grandes bancos del mundo como Goldman Sachs, Barclays, JP Morgan, BBVA entre otros, unieron fuerzas para desarrollar su propia red BlockChain para agilizar las transacciones y transparentar sus operaciones ante el mundo.[9] IBM actualmente esta trabajando con bancos centrales de países como la Reserva Federal de los Estados Unidos para convertir las monedas nacionales en monedas digitales apoyadas por una red BlockChain, pero agregando esas monedas a la oferta monetaria, como un bitcoin inflacionario.[10]

5.1. Plataformas ya desarrolladas en Ethereum

- Augur: Un sistema de predicción financiara descentralizada donde la reputación de los corredores prima sobre el curriculum.[1]

[1] http://www.augur.net

- BoardRoom: Una aplicación de gobierno corporativo basado en BlockChain para implementar sistemas de votación, comunicaciones seguras para evitar espionaje corporativo y manejo del presupuesto.[2]

- Colony: Es un servicio de creación de empresas distribuidas, donde contratos inteligentes se encargan de ejecutar todas las estrategias de negocios, otorgando las recompensas a las personas que mas contribuyan al negocio con su trabajo, determinado por los contratos inteligentes. Utiliza una criptomoneda propia llamada Nectar.[3]

- DIGIX: Plataforma digital de certificados de propiedad. Utiliza los contratos inteligentes de Ethereum que proveen un marco legar y criptograficamente vinculantes de propiedad física de oro u otros commodities actualmente bajo la custodia de un guardián registrado también en DIGIX. También provee un historial completo de la cadena de control, desde el vendedor original, el custodio y todos los reportes de auditoria. [4]

6. CONCLUSIONES

En el nacimiento de la internet vimos como las distancias se acortaba exponencialmente. La distribución del conocimiento humano alcanzaba la globalización por primera vez en la historia. Ya no era necesario viajar largas distancias para consultar un libro o asistir a una reunión con personas que pensaran igual, todo quedaba ahora a un click de distancia: Era el nacimiento de la descentralización, específicamente del conocimiento.

Gracias a esa descentralización de conocimiento, llega una nueva tecnología que promete un cambio aún mas radical: BlockChain. El primer problema que soluciona esta tecnología es el motor de toda revolución pacifica: Las finanzas.

Desde el siglo XVIII, con la creación del primer banco central del mundo, el Sueco, hasta nuestros días, la oferta monetaria estaba controlada por los bancos centrales, creados para financiar guerras y controlar el dinero dentro de un territorio. Este férreo control del principal medio de intercambio creaba problemas como la inflación en países con desesperada necesidad de financiamiento barato.

Bitcoin nace para resolver esto, descentralizando la creación de una moneda de intercambio. Los efectos del Bitcoin no tardaron en verse y hoy hasta bancos privados lo están desarrollando para agilizar sus negocios.

Pero la tecnología BlockChain tiene una infinidad de aplicaciones mas allá de las financieras. La estructura básica de la sociedad moderna se verá afectada por esta nueva tecnología.

Las viejas concepciones de organizaciones verticales van desapareciendo para dar lugar a nuevas formas de organización mas amplias, globales y de responsabilidad distribuida.

Las plataformas como Ethereum aceleran esta revolución pacifica de la descentralización, permitiendo que se desarrollen aplicaciones o plataformas enteras sobre su red, junto con agentes y contratos inteligentes, permiten prescindir de muchos de los sobre costos impuestos por la centralización como la impartición de medidas judiciales o resolución de disputas, tareas exclusivas de los gobiernos, ahora son completamente privatizables.

Así, la tecnología BlockChain cumple con el cometido de toda tecnología: Incrementar el bien estar humano, reducir o eliminar costos económicos y humanos, y ser completamente libre de controles arbitrarios. .

[2]http://boardroom.to

[3]http://colony.io

[4] https://dgx.io

Referencias

[1] Joshua A.T. Fairfield: *Smart Contracts, Bitcoin Bots, and Consumer Protection,Washington and Lee University School of Law 2014*

[2] Dr. Gavin Wood: *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER 2014*

[3] Ahmed Kosba, Andrew Miller, Elaine Sh,i Zikai Wen, Charalampos Papamanthou:*Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, University of Maryland and Cornell University 2015*

[4] Pedro Franco:*Entendiendo Bitcoin :Criptografía, Ingeniería y Economía 2014.*

[5] ÁNGEL HERRERO CRESPO, IGNACIO RODRÍGUEZ DEL BOSQUE y ANDREA PÉREZ RUIZ: Tarjetas de fidelización en el comercio minorista 2009

[6] Nick Szabo:*The Idea of Smart Contracts 1997*

[7] Blas de Lezo:*Las consecuencias de no entregar un conocimiento de embarque 2011*

[8] SF du Toi:THE EVOLUTION OF THE BILL OF LADING 2005

[9] JEMIMA KELLY:Nine of world's biggest banks join to form blockchain partnership, Reuters 2015

[10] GERTRUDE CHAVEZ-DREYFUSS:IBM looking at adopting bitcoin technology for major currencies 2015