La economía de BLOCKCHAIN

Los modelos de negocio de la nueva web

Joaquín López Lérida
José Juan Mora Pérez

kolokium

La economía de Blockchain

Los modelos de negocio de la nueva web

Joaquín López Lérida
José Juan Mora Pérez

La economía de Blockchain

A lo largo del libro se han utilizado varios nombres que corresponden a marcas registradas por organizaciones o personas, por claridad en el texto se ha eliminado el símbolo ®, aunque los autores reconocen que son marcas registradas y usadas por su propietarios, así como la intención de no infringirlas.

Para la elaboración del contenido de este libro, los autores han tomado especial cuidado para asegurar la veracidad y corrección de todo el material expuesto. Los autores no asumen ninguna responsabilidad sobre los daños o perjuicios que el uso o mal uso de la información contenida en este libro pueda ocasionar.

ASIN: B01D03T220

Diseño de la cubierta: © arsbinaria.com

A Abel, te estábamos esperando.

Joaquín López

Para Lola y Pedro,

con la gratitud de un hermano

José Juan Mora

Índice de contenido

Sobre los autores

Joaquín López Lérida
(https://es.linkedin.com/in/joaquinlopezlerida/) Doctor en Informática e Ingeniero de Telecomunicación. Fundador y CEO de la empresa Kolokium, pertenezco al consejo de administración de varias empresas centradas en negocio y economía digital. Adicionalmente soy profesor del área de economía digital en la Escuela de Organización Industrial Andalucía, y director del evento TEDxSevilla cuyo objetivo es impulsar la innovación y la emprendiduría en Sevilla. Participo en la actualidad en el asesoramiento y la puesta en marcha de varias startups de naturaleza fundamentalmente digital.

Email: jlopez@kolokium.es

José Juan Mora Pérez
(https://es.linkedin.com/in/josejuanmoraperez) Tengo la enorme fortuna de haber estado los últimos 15 años trabajando en mi hobby, las tecnologías relacionadas con los sistemas de información. De mi pasión por la tecnología y mi afición a la escritura nacieron mis dos libros "Capacity Planning IT: Una aproximación práctica" y "DevOps y el camino de baldosas amarillas". Soy un convencido de que lo realmente importante de la tecnología son las personas y me esfuerzo cada día en promover esta visión antropocéntrica de la tecnología. Actualmente trabajo en Telefónica, soy socio fundador de Kolokium y colaboro con varias startups a las que mentorizo so sobre tecnologías de la información.

Email: jjmora@kolokium.es

Prólogo

Cuando empezamos a escribir este libro nos plateamos un texto introductorio sobre blockchain. La literatura en castellano sobre este tema era escasa y los recursos estaban dispersos por diferentes blogs y páginas web. Aunque se trata de un texto introductorio nos marcamos el objetivo de avanzar las claves de los modelos de negocio que se van a poder poner en marcha a partir de este tecnología en los próximos años. Como el lector podrá comprobar rápidamente, no se trata de un documento técnico, aunque dado el carácter de la propuesta, hemos querido dedicar algunos capítulos a las bases tecnológicas de blockchain con la idea de no dejar el planteamiento de los modelos de negocio en una apuesta meramente teórica de caja negra.

Por tanto, nuestro objetivo ha sido abrir el camino a la monetización de este tecnología, de cómo pueden ser las futuras aplicaciones a las que de lugar y de cómo se van a ir adaptando los entornos del mundo digital que ya son operativos en la actualidad. Finalmente, como ya hemos comentado, pensamos que no podía ser un modelo de caja negra, por lo que hemos decidido introducir conceptos técnicos de alto nivel que permitan vislumbrar si acaso las bases tecnológicas que sustentan los modelos de negocio que se plantean.

El libro no deja de ser una introducción a las tecnologías blockchain y a los modelos de negocio que se plantearán en un futuro que ya está aquí. No es fácil vislumbrar tendencias en un entorno tecnológico que cambia prácticamente a diario, y probablemente habremos cometido errores, pero las pautas evolutivas de los modelos económicos de blockchain pensamos que están planteados en la dirección correcta.

La tecnología blockchain con todo su ecosistema asociado, viene a solventar un problema en origen de Internet como es la confianza en las transacciones y la posibilidad de poner en marcha sistemas de intercambio de activos que no precisen de los procedimientos del mundo real para poder funcionar. A partir de ahí los modelos de negocio y sus posibilidades se multiplican y lo que tenemos en la actualidad apenas si representa vagamente lo que el futuro puede deparar en torno a esta

tecnología.

Centrándonos en la distribución del libro, en la primera parte (capítulos 1, 2 y 3) se han analizado las versiones de blockchain y los modelos de negocio que plantea. El análisis se realiza tomando ejemplos reales que ya funcionan en la actualidad en unos casos y considerando tendencias ya contrastadas en otros cuando lo primero no ha sido posible. En la segunda parte se aborda la tecnología desde un punto de vista sencillo y accesible, con el objetivo de que el lector pueda comprender las bases del funcionamiento. Pensamos que este planteamiento es suficientemente breve y de alto nivel como para hacerlo accesible a cualquier lector y suficientemente documentado a la vez, como para poder abrir la mente al planteamiento y la discusión de los modelos de negocio de blockchain, que en último caso es el objetivo del libro. Esperamos haberlo conseguido. Todos los capítulos se plantean en base a secciones cortas, centradas en un único concepto, con un desarrollo que crece en complejidad, pero que se estructura de una forma lógica y secuencial.

Desde nuestra empresa, Kolokium (www.kolokium.com), trabajamos día a día es las posibilidades de blockchain y los modelos de negocio que plantea, y nuestra sensación es la de haber comenzado un camino que cambiará mucho en el futuro y que crecerá probablemente de forma exponencial para dibujar un panorama web mucho más completo, transnacional y, sobre todo, democrático.

1
¿Qué es blockchain?

¿Cómo se creó?

El origen de blockchain ha estado envuelto en una cierta aura de misterio que seguramente perdurará para siempre aunque en los últimos tiempos se hayan producido revelaciones sobre su autoría de dudosa argumentación, como la realizada por el australiano Craig Steven Wright en mayo de 2016. Desde sus inicios la palabra blockchain ha ido asociada a Bitcoin, ya que Bitcoin fue la primera aplicación a la que dio soporte blockchain.

Su anónimo autor actuaba bajo el pseudónimo de Satoshi Nakamoto. Creó y diseño el protocolo en el año 2009 y permaneció en el proyecto de desarrollo durante 2 años, pasados los cuáles entregó el control del repositorio de código fuente y la clave de alerta de la red a Gavin Andresen, transfirió los dominios relacionados a miembros de la comunidad Bitcoin y abandonó el proyecto para siempre. Andresen gobernó el desarrollo del proyecto hasta abril de 2014 donde cedió el testigo al holandés Wladimir van der Laan para centrarse en otros aspectos del proyecto Bitcoin.

Gavin Andresen, un hombre clave en la historia de Bitcoin. Fuente fotografía cryptochan.org

Nunca se llegó a conocer su verdadera identidad, ni siquiera si se trataba de una sola persona o de un grupo. Lo cierto es que el código generado y la filosofía que hay tras él se considera en la actualidad una creación suprema en el mundo del software y de la economía, hasta el punto de haber sido nominado para el Premio Nobel de Economía 2016 por parte del profesor PhD de finanzas Bhagwan Chowdhry, de la Universidad de California (UCLA). Posteriormente la Real Academia de las Ciencias de Suecia rechazó esta nominación ya que el Premio Nobel no se puede otorgar a una persona anónima o que haya fallecido.

El programador suizo Stefan Thomas analizó en su día los mensajes publicados en el foro bitcoin por Nakamoto, en un número superior a 500, y estableció perfiles de regularidad para el envío de los mismos. De su estudio se puede concluir que tomando como referencia la hora GMT, los mensajes entre las 5am y las 11am eran los menos abundantes, manteniéndose este patrón incluso sábados y domingos. Esto nos lleva a que si Nakamoto dormía como un individuo medio, podríamos pensar en las zonas horarias este y centro de Estados Unidos o partes de América Central, el Caribe y América del Sur.

La perfección del código es un elemento que lleva a pensar que no se trataba de una sola persona. Dan Kaminsky, un investigador de seguridad que analizó el código de Bitcoin, indicó que Nakamoto o era un genio o era un grupo de personas extremadamente inteligentes. Laszlo Hanyecz, antiguo desarrollador del núcleo de Bitcoin y que mantuvo contacto por email con Nakamoto, consideraba que el código estaba demasiado bien desarrollado como para tratarse de una única persona.

Una de las especulaciones más creíbles la realizó la periodista Leah McGrath de la revista Newsweek. El 6 de marzo de 2014 Leah identificó a Dorian Prentice, un hombre de origen japonés con residencia en California cuyo nombre de nacimiento era Satoshi Nakamoto, como el posible autor del código de Bitcoin. Nakamoto trabajó como ingeniero de sistemas en proyectos confidenciales de defensa y como ingeniero informático para empresas de tecnología financiera. Nakamoto,

despedido un par de veces en la década de los 90, creó su propio negocio. Lo que más inclinó a Leah a pensar en este ingeniero como el autor de Bitcoin fue una entrevista que ella misma realizó en la que Dorian afirmaba:

"Ya no estoy involucrado en eso y no puedo discutirlo. Se ha entregado a otras personas. Ellos se encargan de eso ahora. Ya no tengo ninguna conexión."

Dicha publicación generó un gran revuelo con periodistas acampados en las afueras de la casa de Dorian, que negó posteriormente una y otra vez su relación con Bitcoin. En la tarde del día de la publicación, la cuenta de Nakamoto en la Fundación P2P se activaba por primera vez en 5 años con un escueto mensaje que decía: *No soy Dorian Nakamoto*.

Dorian Nakamoto acosado por la prensa en su casa el 6 de marzo de 2014. Fuente fotografía Los Angeles Times.

En mayo de 2016 el australiano de 44 años Craig Steven Wright, cuyo domicilio fue registrado por agentes policiales en diciembre de 2015 tras la publicación por parte de los portales estadounidenses Gizmodo y

Wired de investigaciones diferentes en las que se le señalaba como el creador de Bitcoin, confirmó ser Satoshi Nakamoto o al menos una parte de él.Wright, con residencia en Sidney, habría tenido como compañero de aventuras al americano con residencia en Florida Dave Kleiman, fallecido en abril de 2013. Kleiman fue un reputado programador, autor de numerosos libros y conferenciante en eventos preferentemente relativos a seguridad. En 2007 Microsoft nombró a Kleiman el hombre más valioso del año para seguridad de Windows. Sin embargo la verificación de esta identidad no ha quedado completamente probada por el propio Wright. Dicha demostración se basaba en la firma y verificación de un mensaje utilizando la llave privada del bloque número 1 y del número 9 que fue la primera transacción realizada a HalFinney por parte de Satoshi Nakamoto. El reputado desarrollador Jeff Garzik comentó que la acción de Wright no probaba nada, y el investigador de seguridad Dan Kaminsky realizó una profunda investigación en su blog con el artículo “Validating Satoshi (OrNot)” (https://dankaminsky.com/2016/05/02/validating-satoshi-or-not/) concluyendo que la afirmación de Wright era falsa ya que lo único que había hecho era reutilizar una vieja firma de una transacción bitcoin realizada en 2009 por el verdadero Satoshi. En el mismo artículo Kaminsky afirmaba que para él la afirmación de Wright no era más que una falsa atribución de las muchas que había habido hasta el momento. Sin embargo el hecho de que Gavin Andresen le hubiera creído le hizo realizar una profunda investigación sobre los argumentos presentados por Wright. En publicaciones posteriores en su propio blog, Kaminsky afirmaba que la firma utilizaba por Wright no era más que una firma incluida en las transacciones Bitcoin de Satoshi en el año 2009 por lo que, a su modo de ver, el único objetivo de Wright era engañar a los medios de comunicación para que le atribuyeran de forma fraudulenta la autoría de Bitcoin.

¿Por qué es tan innovador blockchain?

A grandes rasgos, lo realmente innovador de blockchain es que su sistema permite escribir los movimientos de tokens (por ejemplo bitcoins) en un gran libro virtual que funciona a modo de gran fichero de contabilidad para una moneda. Ese libro ha demostrado ser inatacable, y se basa en estar completamente distribuido y ser actualizado constantemente con las nuevas entradas contables que se van produciendo. Esas entradas contables se agrupan por bloques antes de escribirse en el gran libro de contabilidad que es el blockchain. Es decir, blockchain es una especia de gran libro de contabilidad que puede ser escrito por cualquier entidad, pero que una vez escrito no hay forma de modificarlo, aunque cualquiera puede leerlo.

La unión de los bloques en los que se agrupan los apuntes de contabilidad es lo que se conoce como cadena de bloques o blockchain. Es decir, el blockchain es un gran libro de contabilidad que se va incrementando conforme se van produciendo movimientos y que se caracteriza porque una vez que se crea un movimiento de tokens (un tipo de token es bitcoin) y se inscriben, este movimiento nunca podrá ser modificado por nadie, lo que le da legitimidad y la posibilidad de gestionar transacciones entre personas que no se conocen a través de redes que son inseguras de forma nativa.

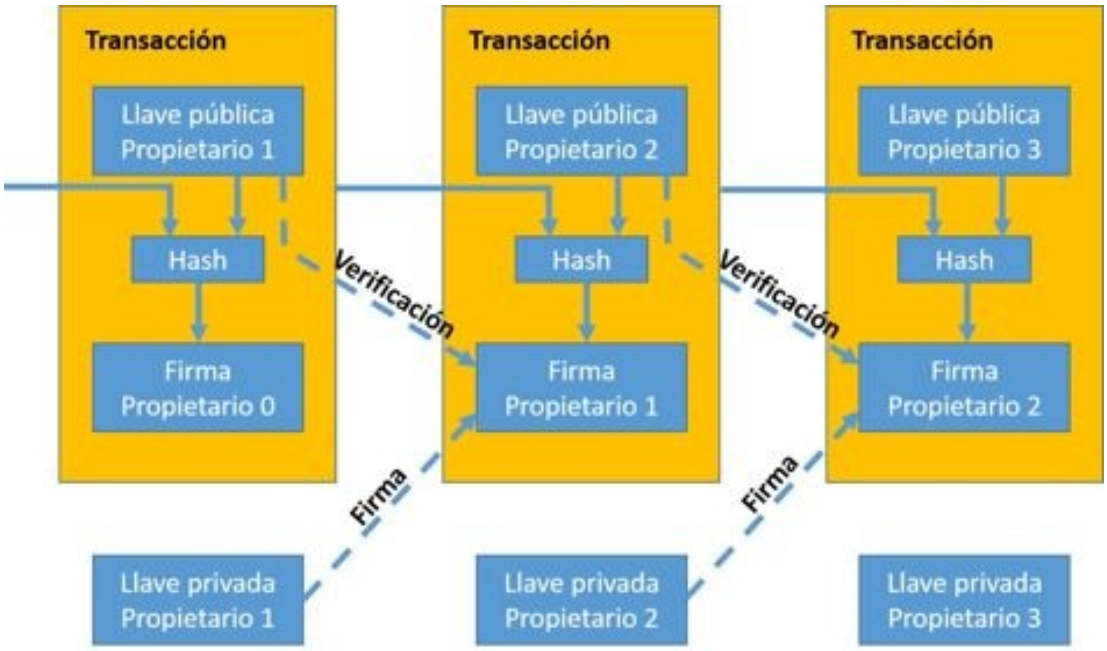


Diagrama blockchain extraído de la publicación original de Satoshi Nakamoto

A nivel general se puede decir que blockchain viene a arreglar un defecto en origen de Internet. Nunca fue una red pensada para intercambiar algo que no fuera información. Es decir, Internet ha conseguido, sobre todo con la llegada de la web 2.0 en el año 2004, optimizar el intercambio de información entre iguales. Lugares como YouTube, Wikipedia, Amazon o Google constituyen repositorios de información de diverso tipo como nunca antes se había conocido. Sin embargo Internet siempre ha carecido de medios de pago, estructuras corporativas, formas de asociación y muchas otras más cosas que siempre han invalidado la separación del mundo digital del mundo real. Mientras que el mundo real no necesita esencialmente al mundo digital para gestionar sus entidades de confianza sobre las que se asienta su modo de operación, el mundo digital necesita imperiosamente del mundo real para gestionar esas entidades de confianza porque las mismas son imposibles en la actualidad. El mundo digital de Internet y sus potentes modelos de negocio no tiene monedas propias, no tiene notarios propios y en definitiva no tiene sistemas de verificación de la información propios. O al menos no los tenía hasta ahora.

De hecho, el mundo digital sólo hacía hasta el momento una cosa bien: gestionar información. Sin embargo hay un buen número de cosas que no sabe hacer, como por ejemplo operaciones relativas a pago,

constitución y formalización de empresas, identificación de personas, etc. Como el mundo digital no sabe hacer esto bien, las ha tomado siempre del mundo real. En Internet pagamos con dinero fiat (dinero convencional) o con medios de pago convencionales como son las tarjetas de crédito o el propio Paypal que no es más que una pasarela del dinero fiat al mundo digital. Se utilizan empresas constituidas en el mundo real, en nuestros registros mercantiles, y se valora a las mismas utilizando medios convencionales como son los índices bursátiles. De hecho se valoran a las empresas con rondas de inversión utilizando medios convencionales basados en reuniones de potenciales inversores y financiaciones convencionales de las entidades bancarias. El mundo digital lo podía hacer mejor y blockchain es seguramente la respuesta.

La historia ya se vivió con el paso de web 1.0 a web 2.0. En la web 1.0 los suministradores de contenidos eran básicamente los medios y la comunicación unidireccional. La web 2.0 protagonizó la revolución de los contenidos con la llegada de los consumidores. El usuario generaba el contenido. De esa manera lugares como YouTube son capaces de generar 350 horas de vídeo por minuto o Wikipedia convertirse en la enciclopedia con más contenido y nivel de actualización de la historia. Ningún medio podría haber logrado por sí sólo un avance en contenidos de este tipo, ni siquiera un país. El poder de los usuarios de Internet lo ha conseguido sin que nadie se haya dado cuenta del esfuerzo realizado.

La nueva web que trae blockchain hará lo mismo con los medios de pago y la estructura de las empresas. El mundo convencional difícilmente es capaz de invertir o financiar empresas que estén en la red. En la actualidad conseguir financiación para una empresa digital que esté comenzando un proyecto es terriblemente complicado por no decir prácticamente imposible salvo que se produzcan situaciones muy favorables que ocurren muy pocas veces. Esta operación que resulta tan compleja en el mundo real, empieza a producirse en el mundo digital con asombrosa facilidad. De igual forma, utilizando las estructuras seguras e inviolables en la actualidad de blockchain, la constitución de empresas con entidad digital, accionistas o la misma contratación de empleados de forma segura y garantizada sin el respaldo de ningún estado empieza a ser ya una realidad. Este libro trata de explicar esta nueva realidad que va a protagonizar una revolución en el mundo digital en los próximos

va a protagonizar una revolución en el mundo digital en los próximos años, pero que poco a poco va a ir cambiando las estructuras y el funcionamiento de muchas entidades del mundo real como se explica en el capítulo 3 dedicado a Blockchain 3.0.

Terminología

Blockchain trae bastantes nuevos conceptos que conviene aclarar cuanto antes para que la lectura del libro se pueda realizar de la forma más didáctica posible. Con independencia de que algunos términos de los que se van a definir a continuación no les resulten familiar, recuerde esta sección para volver atrás cuando tenga dudas sobre algunos términos que se utilizan a lo largo del libro y sobre todo trate de leerlos y asimilarlos aunque sólo sea de una forma básica:

- **Altcoins**.- Son monedas alternativas a bitcoin. Existen más de 600 en la actualidad. Las más destacadas son el Ether, Ripple, Litecoin, Dash y MaidSafeCoin. En la dirección http://coinmarketcap.com/ puede encontrar una lista actualizada de las mismas.
- **Bitcoin** (B mayúscula).- Bitcoin es una aplicación descentralizada (o dApp) que se encarga de desarrollar los mecanismos software que permiten introducir las transacciones de sus tokens en su blockchain particular. Los tokens de Bitcoins se llaman bitcoins.
- **bitcoin** (b minúscula).- Es el nombre que recibe el token que utiliza la dApp Bitcoin para operar sobre su blockchain.
- **Blockchain**.- O cadena de bloques es un registro público que contiene todas las transacciones realizadas con un token determinado como puede ser bitcoin que es el más conocido. Es importante resaltar que es público, por lo que cualquiera puede consultarlo. Se forma a base de bloques. Cada bloque contiene una serie de transacciones de tokens. Mediante algoritmos criptográficos, en el momento que se genera un bloque nuevo, éste se une al último bloque añadido y se vincula de forma irreversible. Nadie puede alterar un bloque con todas sus transacciones una vez añadido, y nadie puede alterar la secuencia y unión de los bloques. El bloque inicial se denomina bloque génesis y es el que genera el nacimiento de cualquier blockchain asociado a un token. El blockchain para cada token es único. Por ejemplo solamente existe un blockchain de bitcoin, que cualquiera puede leer pero que nadie puede alterar. Cada vez que se producen un conjunto de

transacciones, éstas se agrupan en un bloque y se añaden al blockchain de bitcoin como último bloque. En Bitcoin se añade un bloque cada 10 minutos aproximadamente aunque hay otras monedas como litecoin que añade uno cada dos minutos.

- **Bloque génesis**.- El primero de los bloques que forma cualquier blockchain.
- **BTC**.- Abreviatura habitualmente utilizada para referirse al bitcoin.
- **Cartera**.- Una forma de guardar bitcoins o cualquier otra criptomoneda para un uso posterior. Una cartera guarda la llave privada asociada a la dirección de la criptomoneda. El blockchain es el registro de las cantidades de criptomonedas asociadas con esa dirección.
- **Crowdsale**.- Venta pública de tokens que se realiza de una dApp para su puesta en funcionamiento. Lo habitual es que se pongan a la venta un porcentaje del total de tokens de una dApp quedando el resto en manos de los promotores y desarrolladores de la misma.
- **DAO/DAC**.- Por *DescentralizedAutonomousOrganization / Corporation* es el nombre asociado al tipo de empresas que utilizan blockchain como forma de funcionamiento. Estas empresas, como se verá más adelante, tienen sus propias reglas y formas democráticas de obtener consenso. No existen en ningún registro mercantil ni son parte de ningún estado. Sólo existen en Internet, aunque después puedan adquirir una figura jurídica convencional.
- **dApp**.- Pronunciado como “di-app” es una aplicación descentralizada que utiliza un token como activo de cambio para la gestión de sus transacciones. Para que una aplicación sea una dApp debe cumplir varias condiciones que se verán más adelante y a su vez existen dApps de tipo I, II y III según cómo utilicen sus tokens y el blockchain asociado.
- **DAS**.- Por *DescentralizedAutonomousSociety*, suponen un paso más allá de las DAO/DAC ya que tienen mecanismos propios de gestión y operación y no precisan de intervención humana para su trabajo diario. Se habla también de las DAS como empresas autónomas.
- **GH/S**.- Gigahashes por segundo. La unidad en que se mide habitualmente el número de intentos de hash por segundo que un

ordenador puede generar para descifrar un bloque. Más hashes proporcionan más opciones de descifrar un bloque antes que los demás.

- **Hash**.- Es un proceso matemático que utiliza una cantidad de datos variable y produce una salida mucho más corta de longitud fija. Una función hash tiene dos características importantes: matemáticamente es extremadamente complicado conocer los datos de entrada conociendo solamente los de salida y variando una parte mínima de los datos de entrada se obtienen unos datos de salida completamente diferentes.
- **Minería**.- Acción de procesamiento de transacciones realizada para cualquier blockchain por parte de nodos formados por ordenadores. La minería es lo que permite que los blockchains vayan añadiendo bloques conforme se van produciendo transacciones. Los mineros que son capaces de añadir los bloques con más rapidez son premiados con tokens de ese blockchain. Por ejemplo en la actualidad cuando un minero descifra un bloque de Bitcoin y lo añade a su blockchain es premiado con 25 bitcoins.
- **Monedas coloreadas**.- Una funcionalidad añadida a Bitcoin que permite que los bitcoins tengan atributos adicionales. Estos atributos son definidos por el usuario y permiten que determinados bitcoins puedan referirse a otro tipo de activos lo que extiende las funcionalidades del propio protocolo Bitcoin.
- **Satoshi**.- La subdivisión mayor que existe de un bitcoin. Un satoshi es igual a 0,00000001 bitcoin.
- **Satoshi Nakamoto**.- Anónimo inventor del protocolo Bitcoin que dejó el proyecto en el año 2010.

El ecosistema de blockchain

Aunque intuitivamente se pueda pensar que blockchain es una tecnología válida para gestionar y realizar pagos a través de Internet utilizando moneda virtual, eso es sólo el principio del ecosistema y de las posibilidades que permite blockchain.

En realidad se puede pensar en blockchain como un entorno de desarrollo de aplicaciones descentralizadas sobre una base de datos de contabilidad segura y pública, que puede utilizar sus propios recursos para autofinanciar su funcionamiento y que a su vez permite la creación de empresas o agrupaciones de carácter totalmente digital con un sentido muy desarrollado de la democracia y de la participación de los usuarios que las componen.

La razón de todo lo comentado anteriormente es que blockchain lo que permite básicamente es la generación de un entorno de confianza entre pares que elimina la necesidad de intermediarios y que es soportado por toda la comunidad. Este entorno de confianza permite el intercambio de activos de cualquier tipo, no sólo moneda virtual. Bitcoin, la primera aplicación desarrollada para blockchain, permite el intercambio de un token o moneda virtual denominada bitcoin, pero hay otras aplicaciones que permiten el intercambio de otros activos como nombres de dominio, propiedades, oro, etc. El intercambio viene definido por un sentido de la propiedad totalmente definido ya que todo queda almacenado en los blockchain particulares que una vez escritos resultan inalterables, pero que permiten de forma permanente la lectura pública de sus datos.

Así, mientras que la versión 1.0 de blockchain se ha utilizado prioritariamente para la descentralización de dinero y para pagos, la versión 2.0 se va a utilizar para la descentralización de mercados y contempla la transferencia de prácticamente cualquier tipo de activo más allá del intercambio monetario. Las aplicaciones que se están creando, similares a Bitcoin, servirán para la transferencia de cualquier tipo de activo que se podrá agrupar o dividir en función de los movimientos que se vayan haciendo.

El blockchain 3.0 actualmente es más un proyecto que una realidad. Su objetivo será transformar una gran parte de las actividades humanas abarcando aspectos como la salud, el gobierno o la educación, transformando su forma de funcionamiento y diseñando entornos abiertos y privados a la vez, con acceso democrático a la información y con innumerables posibilidades para la industria y la sociedad. Blockchain 2.0 es una evolución de los servicios, fundamentalmente digitales hacia un entorno más seguro y funcional, blockchain 3.0 es una revolución que afectará globalmente a los servicios que sustentan nuestra sociedad.

Por ejemplo la empresa slock.it es una innovadora startup que utiliza blockchain para la gestión de la apertura y cierre de puertas. Con slock.it se podrán programar puertas utilizando su blockchain para que un determinado usuario las pueda abrir una serie de días concretos y otros no. Esto permitirá que las puertas se puedan programar a distancia y reconozcan las personas con autorización para abrirlas o cerrarlas. En la actualidad sclock.it se encuentra en negociaciones con varias organizaciones para la implantación de estas cerraduras en casas de alquiler.La aportación de blockchain a los sistemas de alquiler estará en que una vez que se formalice el pago de un alquiler, la puerta queda automáticamente programada para abrirse con ese usuario durante el período de alquiler, y solamente para ese usuario. Ni siquiera el propietario podrá abrir la puerta durante ese período de alquiler. La identidad del usuario que puede abrir la puerta queda almacenada en el blockchain de slock.it. Cada vez que un propietario de una puerta quiera utilizar la tecnología de slock.it para sus puertas, tendrá que comprar tokens de sclok.it para hacer viables las transacciones dentro del blockchain que utilizan. El hecho de que un usuario compre tokens de slock.it hará que estos puedan experimentar cambios de valor y por tanto los poseedores de tokens, que son formalmente los accionistas de la empresa, podrán ver incrementado el valor de los mismos.

Todo este conjunto de transacciones genera un ecosistema donde una empresa crea una aplicación que funciona sobre un blockchain con unos tokens que son necesarios para la utilización de esa aplicación (formalmente una aplicación descentralizada o dApp). Si la aplicación de

(formalmente una aplicación descentralizada o dApp). Si la aplicación de la empresa tiene éxito los usuarios empezarán a comprar tokens para poder utilizarla lo que generará un mercado similar al bursátil que permitirá que las dApp más populares sean cada vez más valiosas. Estas dApps van a ser propiedad de las DAOs o DACs (después se comentarán con más detalla). Las DAOs o DACs son el embrión de las empresas digitales que crean dApps. Un concepto más avanzado serán las DAS (DistributedAutonomousSocieties), que serán sociedades que agrupan DACs o DAOs y que permitirán desarrollar de forma automática la gestión del funcionamiento de forma que las mismas estarán activas y en funcionamiento sin necesidad de la intervención humana. Estas sociedades basarán todo su funcionamiento en la utilización de uno o varios contratos que permitirán gestionar su propia economía, contratar trabajadores y pagarles con sus propios tokens y gestionar todas sus operaciones de forma automatizada.

Todo lo explicado con anterioridad se desarrolla completamente en el mundo digital de una forma segura y descentralizada. Es decir, no hay ninguna dependencia del mundo real ya que los tokens o monedas que son la gasolina de las dApps, no están reguladas ni reconocidas en el mundo real, tampoco lo están las empresas (DAOs o DACs). A pesar de todo lo anterior, funciona, genera valor y permite establecer transacciones y desarrolla de una forma completa el sentido de la propiedad tal cual la conocemos en el mundo real.

Este nuevo ecosistema está conectado con el mundo real y hoy en día es posible realizar transferencias de dinero fiat por tokens de los diferentes blockchains que están en funcionamiento en lugares como Localbitcoins (http://www.localbitcoins.com), Ripio (http://www.ripio.com), Bit2me (http://www.bit2me.com), Coinbase (http://www.coinbase.com), etc. Estos tokens se aprecian y deprecian permanentemente con respecto al dinero fiat en función del valor de las dApps que representan.

Por ejemplo un bitcoin tiene un valor en la actualidad de unos 340€ que puede ser convertido en cualquier momento y un Ether tiene un valor de unos 12€. Esto se debe a que sus dApps asociadas (Bitcoin y Ethereum) van siendo reconocidas y por tanto han ido adquiriendo valor en los últimos tiempos.

Evolución de la cotización del Bitcoin y capitalización

Cuando una dApp va a salir oficialmente al mercado se organiza una especie de subasta de tokens por un valor fijo que después irá fluctuando en función del valor de esa dApp. La acción de salida y venta de tokens de una dApp se denomina crowdsale (venta multitudinaria).

A diferencia del mundo real, las crowdsales pueden generar importantes beneficios (y pérdidas) para las personas que deciden adquirir tokens. Si usted hubiese adquirido tokens de la primera crowdsale que se produjo, la de Bitcoin, podría haber adquirido bitcoins al precio 0,10€ en octubre de 2010. En la actualidad esos bitcoins valen 340€.

El problema del 51%

Todo el mecanismo que tiene una dApp para su funcionamiento tiene un punto débil que se conoce de antemano y de difícil resolución: el problema del 51%.

Para cualquier dApp un teórico usuario que poseyera el 51% de la misma tendría el control total, sobre todo en las dApps con mecanismos de funcionamiento basados en POS, ya que la decisión se toma en función del grado de participación. Pero incluso en el caso de las POW, el problema no está completamente en el gobierno de las decisiones, sino en el alojamiento del blockchain asociado a esa dApp.

Cuando un usuario posee más del 51% de los nodos de una dApp, tiene poder teórico para cambiar el contenido del blockchain asociado a esa dApp ya que en el fondo un blockchain funciona por consenso de los nodos que los poseen. Si más del 51% de los nodos mineros de un blockchain dicen que la información que contiene dicho blockchain debe ser A, aunque la verdadera sea B, el resto de nodos cambiarán a A porque esa es la opinión de la mayoría de los nodos.

Aunque esta posibilidad es una realidad y un claro punto débil (tal vez el único) que presentan los protocolos que utilizan blockchain, la posibilidad de que esto ocurra es realmente baja por los siguientes motivos:

- Si se trata de una dApp pequeña, lo normal será que si alguien tiene más del 51% de esa dApp éstos sean sus creadores originales. No parece que pueda tener mucho interés para los creadores originales de una dApp alterar el contenido de la misma y cambiar la realidad. Esto desacreditaría a la dApp (el resto de usuarios se quejarían) y la haría fracasar con seguridad. No parece que para una dApp que está comenzando y tiene poca distribución de tokens, resulte interesante falsear la información de la misma por parte de sus creadores.
- En el caso de las dApps que son más grandes, como es el caso de Bitcoin, el interés por alterar el contenido del blockchain asociado

puede ser bastante interesante para un teórico ladrón. Si alguien es capaz de cambiar el contenido del blockchain de Bitcoin, aunque fuera sólo en unas líneas, podría anotar transferencias verificadas por unos cuantos miles de bitcoins que significarían una cantidad importante de dinero. Para que alguien pudiera realizar tal hazaña, necesitaría poseer al menos el 51% de la capacidad de cómputo que tiene la red Bitcoin en la actualidad. Pero esta acción implicaría en la actualidad una inversión tan descomunal que sería mucho más económico emplear esos recursos en trabajar bajo las reglas del protocolo y obtener las recompensas por el descifrado de bloques.

Con todo lo anterior, no es descartable en el futuro que algún gobierno o gran organización quisiera acometer tan descomunal empresa con un objetivo no económico, sino destinado a sembrar la desconfianza y destruir la red.

En palabras de Gavin Andresen, uno de los líderes del proyecto:

Algo que un "atacante del 51%" puede hacer es evitar que otros acepten nuevas transacciones que no sean las del atacante. Esto detendría el procesamiento de pagos e inutilizaría la red. Pero también sería obvio que tal cosa está ocurriendo. Por eso, defender a la red de un ataque del 51% es fácil:

Puede obligarse al atacante a contar simultáneamente con un gran poder computacional y con una gran cantidad de bitcoins antiguos, de alta prioridad, para sostener su ataque. Así, rápidamente se quedaría sin bitcoins de alta prioridad, y se vería obligado a incluir transacciones de otros o bien sufrir el rechazo de su cadena.

El código ya incluye una noción de "prioridad", que utiliza para prevenir el spam de transacciones (enviarse a sí mismo miles y miles de pequeñísimas fracciones de bitcoin, con la intención de que

todos los demás hagan el trabajo de validación y almacenamiento). Extender eso para influir en el código que selecciona el fork de la cadena de bloques no es difícil.

Puede que lo haga y lo mantenga como una opción a ser utilizada sólo en caso de emergencia.

El blockchain de Ethereum

Como se ha comentado anteriormente, hay varios tipos de blockchains que se corresponden con los tokens de tipo 1. El blockchain más popular es el de Bitcoin. Sin embargo este blockchain tiene demasiadas limitaciones en el sentido de que es difícil desarrollar aplicaciones por encima del mismo.

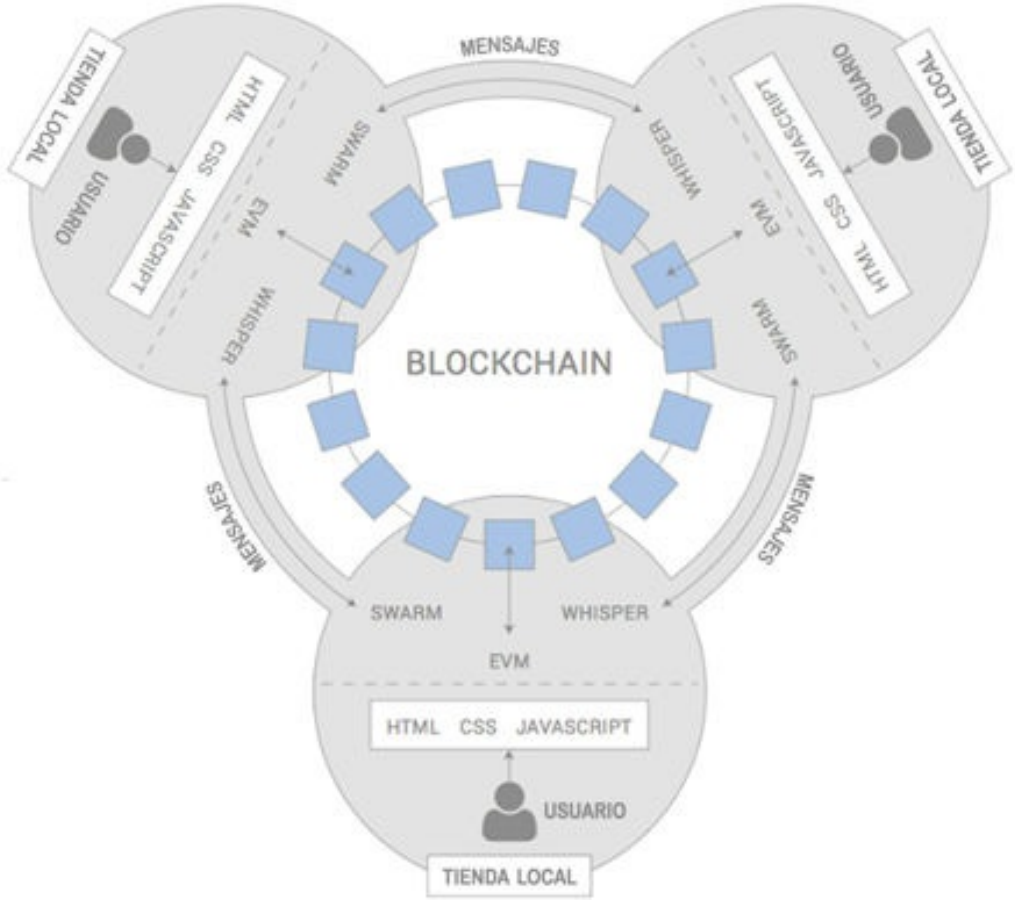
Frente a esta limitación surgió a finales de 2013 el blockchain de Ethereum. Su autor, Vitalik Buterin lo describió inicialmente como un entorno de computación cuyo objetivo era el desarrollo de aplicaciones descentralizadas sobre un blockchain. Ethereum cambió muchas cosas durante ese año porque aunque habían surgido numerosos proyectos de aplicaciones descentralizadas, todos eran del tipo bitcoin 2.0 (utilización del blockchain de Bitcoin). Sin embargo Ethereum utilizaba su propio blockchain y a su vez proporcionaba un potente entorno de computación. En muy poco tiempo Ethereum se convirtió en una valiosa herramienta que se encargaría de llevar las funcionalidades del blockchain más allá del puro intercambio económico. En julio de 2014 Ethereum obtuvo una financiación por mecanismo de crowdsale de 18,5 millones de dólares y finalmente, tras no pocas dificultades, lanzó su blockchain el 30 de julio de 2015.

El token que utiliza Ethereum se denomina ether. El ether es una criptomoneda más. A abril de 2015 el ether es la segunda criptomoneda por capitalización en el mercado tras bitcoin, con una volumen de 627 millones de dólares y un valor de 10 dólares por cada ether. Son números todavía pequeños en comparación a bitcoin, que tiene una capitalización en mercado de 6.561 millones de dólares, pero en poco tiempo se ha convertido, sin ninguna discusión, en la segunda criptomoneda por encima de Ripple (209 millones de dólares) o Litecoin (148 millones de dólares).

Ethereum utiliza para su funcionamiento la dAppSwarm (no confundir con la criptomoneda del mismo nombre) para realizar el almacenamiento distribuido y la dAppWhisper para la gestión de mensajería descentralizada.

A grandes rasgos se puede decir que Swarm en un protocolo que permite la ejecución de los smart contracts de Ethereum con independencia del medio específico de almacenamiento. Sería el BitTorrent que permite el desarrollo del protocolo P2P de intercambio de ficheros.

Por otra parte Whisper permite el intercambio de mensajes utilizando la misma red que utiliza el blockchain. Es un protocolo que está separado de forma lógica del blockchain. El uso de Whisper no es obligatorio, pero tiene numerosas aplicaciones como la publicación de información entre dApps, la colaboración para transacciones complejas cuando están presentes varias dApps, etc.



Los tres componentes de Ethereum trabajando juntos

La base de Ethereum son los smart contracts (contratos inteligentes) que son transacciones programables que se pueden realizar sobre su blockchain con bastante facilidad. Sin pérdida de generalidad podemos asociar la idea de smart contract con la de dApp. De las dApp y sus características se habla con detalle en el siguiente capítulo.

Smart Contracts

La forma de entender mejor el concepto de un smart contract en Ethereum es el de una máquina de bebidas. Cuando se introduce una moneda en la máquina por el valor de una bebida, la máquina ejecuta un código de forma inexorable que acaba finalmente con la provisión de la bebida. En el caso de esta máquina, si no se deposita el precio de la bebida no se detona el evento que hace que podamos tener acceso a la misma. En caso de que depositemos la cantidad necesaria, la provisión de la bebida de realiza de forma automática. No hay intervención humana, no hay diálogo posible, no hay precio negociable. Si se cumplen las condiciones la bebida se obtendrá, si no se cumplen es sencillamente imposible.

La idea de un smart contract es exactamente eso, son aplicaciones programables que permiten la ejecución automática de tareas utilizando el blockchain de Ethereum. Estos contratos se ponen en marcha cuando se producen determinados eventos y utilizan el blockchain de Ethereum como la fuente de datos para realizar las transacciones para las que están programados. Lo smart contracts de Ethereum se pueden realizar en varios lenguajes y compilarse posteriormente para la máquina virtual de Ethereum (EVM – Ethereum Virtual Machine) antes de ser depositados en la blockchain.

Ethereum utiliza un mecanismo denominada *gas* para limitar el tiempo de ejecución de estos contratos. Cada contrato debe pagar una cierta cantidad de gas por su computación. A mayor tiempo de computación mayor gas tendrá que emplear. Hay que considerar que la ejecución de contratos en Ethereum es cara ya que debe ser ejecutada en cada nodo completo de Ethereum. La idea tras el gas es limitar la posibilidad de loops infinitos en contratos que hicieran caer la EVM. Un gas es equivalente aproximadamente a 0.00001 ether y permite la ejecución de una línea de código o un comando. Cuantas más líneas de código tenga un contrato más cara será su ejecución y por tanto más gas habrá que pagar por cada ejecución. Por ejemplo, si A quiere enviar 1 ether a B, en realidad A tendrá que enviar 1.00001 ether para hacer posible la

transacción ya que el coste de transferir ethers es de 1 gas al tratarse de una operación muy simple de un solo comando. Hay contratos en Ethereum que precisan de cientos o miles de gas para poder ejecutarse. Si A quiere ejecutar un contrato en Ethereum que está asociado a una dirección B y no incluye el suficiente gas en las transferencia, ésta no se realizará y por tanto no se hará efectiva al acción del contrato.

A nivel de Ethereum un contrato queda vinculado a una dirección del blockchain una vez que son compilados y enviados. Cuando se produce cualquier evento que esté contemplado en el contrato, se enviará la transacción correspondiente a la dirección y la EVM de Ethereum ejecutará la programación asociada a dicho contrato utilizando los datos que hayan sido enviados.

Los contratos pueden ser tan simples y tan complejos como lo determine su programación. La única diferencia sustancial es que los contratos más complejos requieren más gas para su ejecución. En principio cualquier tipo de operación que pueda ser vinculada a la automatización permite un contrato: votos, apuestas, compras digitales, préstamos, etc.

Por último aclarar que aunque los smart contracts se han convertido en una seña de identidad de Ethereum, no son exclusivos de este blockchain. Otras blockchain que permiten la ejecución de estos contratos son BitHalo(https://bithalo.org/), Codius (https://codius.org/), Counterparty (http://counterparty.io/) o RootStock (http://www.rootstock.io/).

Algunos tipos de smart contracts

En la actualidad se utilizan contratos inteligentes para muchas operaciones diferentes como se comenta a continuación.

Uno de los usos más frecuentes son los préstamos. Un contrato inteligente para préstamos almacena cualquier operación de préstamo con sus condiciones y garantías en la cadena de bloques. Si se efectúa el pago la operación quedará finalizada. Caso de no efectuar el pago según las condiciones establecidas, la propiedad que se establezca como garantía al préstamo quedaría automáticamente transferida. Esta transferencia se podría hacer revocando la llave privada que da acceso a la propiedad y generando una nueva que pasaría a ser propiedad de la cuenta que realizó el préstamo.

Otra posible aplicación serían las herencias. Las mismas se podrían automatizar de forma que cuando el contrato asociado a las mismas certifique un fallecimiento en base al acceso a un registro de personas fallecidas, la propiedad se transfiere a la dirección blockchain receptora de la misma. Esta transferencia se puede hacer igualmente revocando las llaves privadas del propietario original y proporcionando una llave privada nueva al heredero.

Las apuestas o predicciones de mercado son otro tipo de contrato inteligente. Dos partes envían una cantidad al contrato inteligente en base al resultado de una predicción o evento. Una vez que se produce el evento y se obtiene un resultado, el contrato de encargará de transferir la cantidad depositada por las dos direcciones a la dirección que haya acertado en la predicción.

Smart Properties

Prácticamente unido al concepto de smart contract se encuentra el de Smart property o propiedad inteligente. Bajo este concepto se identifica a cualquier tipo de activo, digital o físico, que se puede registrar en blockchain a través de una llave única. El poseedor de esa llave es el poseedor único del activo y transferencias de la llave, por ejemplo a través de acciones que se pueden poner en marcha vía smart contracts, implican transferencias del activo.

De esta manera blockchain se convierte en un sistema de inventariado de activos, gestión y seguimiento de los mismos así como un sistema de compra/venta por el simple hecho de cambiar las llaves que dan acceso a cualquier activo. Esto convierte a blockchain en un sistema descentralizado de intercambio de activos de una forma inmediata a la vez que permite un sistema único de autenticación para el acceso a los mismos.

El único punto a destacar aquí es que no vale para cualquier tipo de activo sino únicamente para aquellos que se identifican de forma única a través de algún tipo de identificación. Es decir, no valdría para activos que se proporcionan de forma masiva sin ningún tipo de identificación, sino para aquellos que tienen asignados un poseedor único, que sería aquel que está en posesión de la llave privada del mismo.

Un ejemplo de este tipo sería everledger (www.everledger.io), un sistema de identificación y seguimiento de diamantes realizado a través de un doble blockchain, el de Bitcoin y el Eris, conformando de esta manera un doble blockchain público y privado a la vez. El API de everledger permite a las empresas el acceso a los certificados sobre posesión de diamantes, así como toda la información relativa a reclamaciones y aspectos legales de una forma única, centralizada y pública para cada diamante en concreto (un activo físico).

2
Blockchain 2.0

Introducción

En las comunicaciones realizada por Satoshi Nakamoto en 2009 con la especificación de Bitcoin, se comentaba lo siguiente:

"…*el diseño soporta una gran variedad de posibles tipos de transacción que diseñé hace años. Transacciones de fideicomisos, contratos, arbitrajes de terceras partes, firmas de varias entidades, etc. Esto son cosas que habrá que explorar con Bitcoin en el futuro, pero deberán estar diseñadas desde el principio para asegurarse que será posible hacerlas..."*

Estas palabras de Satoshi Nakamoto en 2009 suponían el preludio a lo que conocemos como Blockchain 2.0. Si se parte de la base que Blockchain 1.0 está pensado para las transacciones económicas y pagos básicamente, se puede pensar que Blockchain 2.0 está pensado para la gestión y transferencia de activos y cualquier otro tipo de bien que pueda estar en un registro público. Igualmente se puede utilizar para gestión y transferencia de activos físicos siempre que los mimos puedan ser codificados de alguna manera.

Blockchain 2.0 supone el paso de las criptomonedas al mundo de las aplicaciones reales. La base del blockchain 2.0 son los contratos inteligentes que se encargan de ejecutar de forma automática acciones programadas sobre el blockchain que se ejecutan.

Blockchain 2.0 ha traído una nueva ola de aplicaciones descentralizadas o dApps, mucho más sofisticadas que en el caso de la blockchain 1.0 donde estas aplicaciones iban dirigidas exclusivamente a los pagos y transferencias económicas.

Antes de seguir con los conceptos y aplicaciones asociadas a la blockchain 2.0 se introducirá el concepto de dApp. Conviene aclarar que una dApp no es exclusiva de la blockchain 2.0, existen en todas las blockchains, pero su importancia y su conocimiento se ha puesto de manifiesto a partir del nacimiento de la nueva ola de aplicaciones

blockchain y sus características más allá de las transferencias económicas.

Dapps

Las dApps o aplicaciones descentralizadas constituyen una de las partes más importantes del ecosistema de blockchain. Una dApp no es más que un desarrollo software que tiene ciertas peculiaridades como son:

- Debe estar escrita completamente en código abierto y por tanto estar accesible para cualquiera que quiera entender su funcionamiento.
- Las dApps funcionan de manera autónoma, sin la intervención de ninguna persona y sin ninguna entidad que las controle.
- Una dApp adaptará su código y lo actualizará en función de que los propietarios de los tokens de la misma así lo decidan de forma mayoritaria en función de las mejoras que se propongan.
- Una dApp tiene tokens que son la gasolina que las hace funcionar. El objetivo último de una dApp es gestionar las transacciones que se hacen sobre sus tokens sobre una blockchain concreta. Toda aportación de valor que se realiza a la dApp por parte de sus desarrolladores debe ser recompensada en tokens de la misma aplicación.
- Una dApp genera nuevos tokens de acuerdo con un algoritmo estándar criptográfico actuando como una prueba del valor que se está aportando al funcionamiento de la misma.

La primera dApp que se creó fue Bitcoin. Su desconocido inventor, Satoshi Nakamoto, diseñó Bitcoin para permitir el pago electrónico P2P (entre iguales). Este pago electrónico se realiza a través de su token, bitcoin.

La dApp Bitcoin no requiere de ninguna entidad central que la regule y sin embargo ha demostrado ser extremadamente segura y eficaz para permitir el pago. Cualquier usuario que quiera utilizar Bitcoin para realizar pagos a otros usuarios deberá adquirir tokens de Bitcoin, que en este caso son los bitcoins. El valor de la aplicación Bitcoin ha venido determinada por la cantidad de personas que utiliza los bitcoins para

realizar transferencias monetarias. Finalmente esos bitcoins se pueden transformar en dinero fiat a través de las numerosas aplicaciones que conectan el mundo digital como el mundo real.

Existen tres tipos de dApps en función del uso que hagan de sus tokens y del blockchain al que estén asociadas:

- **Tipo I**.- Poseen su propia cadena de bloques como es el caso de Bitcoin. Otras dApps con sus propios blockchains son Ethereum y Litecoin.
- **Tipo II**.- Utilizan blockchains de una dApp de tipo I. Estas dApps son protocolos y tienen sus propios tokens que necesitan para su funcionamiento, pero no tienen un blockchain propio. Por tanto se realiza una equivalencia entre el token de la dApps tipo I sobre la que funcionan y sus propios tokens. El protocolo Omni, que utiliza el blockchain de Bitcoin para gestionar activos y tiene su propia moneda, Mastercoin, es un ejemplo. Este protocolo permite la creación de monedas digitales sobre el blockchain de Bitcoin entre otras funcionalidades. Las carteras de Omni permiten gestionar bitcoins y activos Omni a la vez.
- **Tipo III**.- Utilizan el protocolo de una aplicación descentralizada tipo II. Son también protocolos y utilizan tokens propios que son necesarios para su función, pero no actúan directamente sobre las de tipo I sino que utilizan funciones de tipo II que permiten un desarrollo más rápido y sencillo. La red SAFE que funciona sobre el protocolo Omni es un ejemplo de dApp de tipo III. Esta red utiliza su propia moneda, Safecoin, para operar una red entre iguales de almacenamiento. Si una aplicación quiere utilizar el almacenamiento seguro que proporciona SAFE, debe adquirir Safecoins. Esta red garantiza el almacenamiento seguro de archivos de una manera descentralizada.

dApp	Capitalización ($)
bitcoin	6.927.007.966
ethereum	756.007.381
ripple	216.821.817
litecoin	170.045.506
DASH	43.903.502

Principales dApps con su capitalización en mercado en dólares en mayo de 2016

Por hacer una analogía, podríamos pensar en las aplicaciones tipo I como los sistemas operativos de los ordenadores, las aplicaciones tipo II podrían ser los exploradores como Chrome o Firefox, mientras que las aplicaciones tipo III serían desarrollos web como Amazon, eBay o Google que precisan de los navegadores y desarrollos web para poder funcionar.

Funcionamiento de una dApp

Como ya se ha introducido anteriormente, una dApp no es más que un contrato inteligente cuyo mecanismo de funcionamiento está basado en sus propios tokens que se almacenan en algún blockchain. Por tanto los tokens suponen la gasolina de las dApps y lo que las hace funcionar. Un usuario que no tenga tokens tendrá que comprarlos si quiere utilizar esa dApp. Cuanta más demanda haya de tokens, más valdrán los mismos y por tanto más valor acumularán los poseedores de esos tokens que pondrán vender los mismos o vender la utilización de la dApp.

Por ese motivo, las dApp con éxito conseguirán que sus tokens cada vez valgan más, dando valor a su utilización y generalización. Un ejemplo de dApp con éxito es Bitcoin. En 2013 por ejemplo, un bitcoin tenía un valor de 100$ aproximadamente. En la actualidad, 2016, un bitcoin tiene un valor de unos 340$. Esa apreciación es un indicativo de éxito en la dApp. Cualquier persona que quiera utilizar la dApp de Bitcoin necesita bitcoins, que tendrá que comprar a ese precio a alguno de los poseedores o generarlos mediante minería como se comentaba en el capítulo 1.

Otro aspecto importante en el funcionamiento de una dApp es su gestión. Las dApp son aplicaciones autónomas por naturaleza, es decir, una vez comienzan a funcionar no hay intervención humana más allá de los mecanismos de aprobación de acciones que se establecen. Estos mecanismos de aprobación de acciones determinan en un momento dado qué hacer ante las peticiones de los usuarios y por tanto qué escribir en la blockchain asociada a esa dApp.

Hay dos mecanismos para establecer por parte de los usuarios de una dApp lo que tiene que hacer en un momento dado: la prueba de trabajo (POW o *Proof of Work*) y la prueba de participación (POS o *Proof of Stake*).

- **POW**.- Las decisiones sobre los cambios y la gestión de una dApp se realizan en función de la cantidad de trabajo que cada usuario ha

contribuido para el funcionamiento de la dApp. Este mecanismo basado en POW se llama minería y los usuarios que realizan el trabajo son los mineros. Bitcoin funciona con POW..

- **POS**.- Las decisiones acerca de los cambios en una dApp se realiza a partir de las participaciones (tokens) que los usuarios poseen de esa dApp.

Hay dApps que utilizan los dos mecanismos de forma paralela como es el caso Peercoin (https://peercoin.net).

De una manera u otra, una dApp tiene que ser capaz de distribuir sus tokens. Para esto existen tres métodos: minería (POW), recaudación y el desarrollo de la propia dApp:

- La minería otorga tokens a los usuarios que contribuyen al funcionamiento de la aplicación. De hecho la minería es la forma más común que tienen las dApps para generar nuevos tokens. Por ejemplo en el caso de Bitcoin, cada vez que un usuario es capaz de descifrar un bloque para unir a la cadena de bloques del blockchain de Bitcoin, recibe 25 bitcoins. Como en Bitcoin un bloque se produce cada 10 minutos aproximadamente, la red produce 25 nuevos bitcoins cada 10 minutos, que se otorgan al usuario que ha sido capaz de descifrar el nuevo bloque.
- El mecanismo de recaudación de fondos se suele realizar cuando una dApp va a salir al mercado en lo que sería equivalente a una oferta pública de acciones. Esta oferta pública de acciones se denomina crowdsale. Por ejemplo en el protocolo Master, inicialmente se distribuyeron 100 mastercoins por cada bitcoin enviado a una dirección concreta. Los bitcoins recogidos se utilizaron para financiar el desarrollo inicial del protocolo.
- El tercer mecanismo se utiliza para pagar a los desarrolladores de una aplicación. Siguiendo con el ejemplo de Master, un 10% de los mastercoins generados inicialmente se utilizaron para pagar a los desarrolladores del protocolo Master.

De esta manera cuando una dApp va a salir al mercado se publica un documento con la descripción de la dApp y sus características, se

distribuyen un conjunto inicial de tokens por mecanismo de crowdsale normalmente y se asigna un conjunto de tokens a los desarrolladores de la dApp. Las crowdsales son vitales en la actualidad para el desarrollo de las dApp. De su puesta en marcha y funcionamiento se habla posteriormente.

El resto dependerá de la dApp, su implantación en el mercado y el éxito que tenga. A más éxito de una dApp, más valor tendrán sus tokens y mejor será la inversión y el valor de la posesión. Esto nos lleva a un futuro con dApps donde se establecerá un modelo de pago por uso y donde las dApps tendrán autonomía para autoregularse en función de lo que sus propietarios vayan estableciendo y decidiendo.

DAO/DAC

Las DAO/DAC (DescentralizedAutonomousOrganizations / Corporations) son otro de los entes con un importante protagonismo en blockchain. A grandes rasgos podemos ver los DAO/DAC como dApps con alguna forma de constitución y funcionamiento. Es decir, se puede ver un DAO/DAC como una dApp con una forma más compleja que tiene definida su gobernanza en el blockchain y que posee unos mecanismos para financiar y estructurar sus operaciones.

Es decir, las DAO/DAC están constituidas por una o varias dApps, poseen alguna forma de constitución y gestionan unos tokens que son propios de dicha DAO/DAC. Lo normal es que cuando una DAO/DAC se quiera poner en marcha organice una especie de subasta pública de una parte de sus tokens. Esta subasta pública se denomina crowdsale y es un tipo de contrato inteligente más. En una crowdsale se ponen a la venta un porcentaje del total de tokens previstos para esa DAO/DAC. En general, en función de la recaudación que se obtenga se dividirá el número de tokens de dicha crowdsale por el dinero recaudado y en función de eso se establecerá el valor inicial del token. Los propietarios de esos tokens podrán posteriormente transferir la posesión de los mismos o utilizarlos con la propia aplicación.

Una DAO/DAC puede tener una red descentralizada de agentes autónomos que ejercen trabajos de forma automatizada para permitir que la organización funcione. Estos agentes autónomos son normalmente dApps que están desarrolladas para realizar un trabajo conjunto.

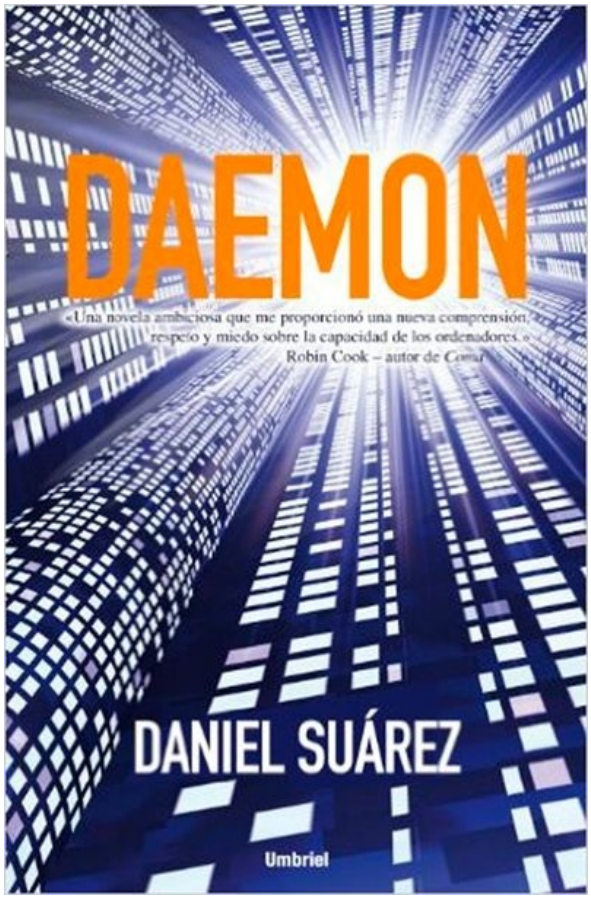
DAS

Un concepto que va más allá de las DAO/DAC comentadas con anterioridad es el de DAS (DescentralizedAutonomousSocieties). Las DAS constituyen asociaciones de conjuntos de dApps, DAOs o DACs se pueden operar de forma autónoma.

La idea de DAS tiene que ver con la puesta en marcha de sociedades que se rigen de forma automática por uno o varios tipos de contratos, que tienen una forma automática de puesta en funcionamiento a través de mecanismo de crowdsale normalmente y que son capaces de pagar dividendos a sus accionistas. Adicionalmente las DAS tienen una estructura socioeconómica embebida de forma automática a su funcionamiento y una estructura política que permite el gobierno de su funcionamiento de forma automática.

Estas asociaciones reciben un feedback automatizado a través de los mercados de predicciones que ya existen y son capaces de tomar decisiones inteligentes en función de su propia evolución o de la evolución de factores externos que pueden ser cuantificados de manera objetiva a través de mercados de predicción. Igualmente los accionistas de estas sociedades, es decir, los poseedores de sus tokens, son capaces de tomar decisiones sobre la evolución de las mismas utilizando voto automatizado que utiliza mecanismos de blockchain. En última instancia estas DAS tienen capacidad de autodisolverse en la eventualidad de determinados sucesos o situaciones de la propia sociedad que han sido previstos en los contratos que las gestionan.

Esto último permitiría evitar situaciones ya descritas en la literatura de ciencia ficción sobre sociedades de este tipo que acaban con la economía mundial por el simple hecho de seguir las directivas con las que habían sido programadas. Una situación de ciencia ficción en el pasado que podría dejar de serlo. El ejemplo anterior se documentó por primera vez en el libro de Daniel Suárez “Daemon” (Umbriel, 2014) donde un software incontrolado tras la muerte de su creador amenaza a la sociedad mundial con destruirla completamente.



Portada del libro "Daemon" de Daniel Suárez

La filosofía tras las DAS es la puesta en marcha de instituciones que podrían funcionar de manera independiente de forma indefinida proporcionando beneficios a sus accionistas y utilizando sus propios tokens como la gasolina de su economía. Estas instituciones tendrían una naturaleza incorruptible ya que su base es un trozo de código más o menos complejo funcionando de forma indefinida, convirtiendo de este modo a la política en un simple problema de ingeniería.

El ejemplo de Namecoin

Namecoin (https://namecoin.info/) es un buen ejemplo sobre aplicaciones blockchain 2.0. El objetivo de Namecoin es desarrollar un sistema de nombres descentralizado o DNS utilizando la tecnología de Bitcoin y permitiendo un control descentralizado del sistema de nombres de dominio. El token de Namecoin es NMC y utiliza un blockchain particular basado en el código de Bitcoin para el almacenamiento de sus registros.Namecoin entró en funcionamiento el 19 de abril de 2011 y tiene una producción máxima de 21 millones de monedas de las que hay disponibles en la actualidad 14 millones con un valor total de algo más de 6 millones de dólares o 14.100 bitcoins.

Namecoin utiliza el dominio .bit, dominio que no está registrado oficialmente por IANA como un gTLD (generic Top LevelDomain). En la actualidad el coste de un dominio .bit es de 0.02 bitcoins o 10 NMC por año. A abril de 2016 existen 583.746 dominios .bit, con 3.847 sitios web dados de alta de los que 280 son únicos, es decir, sólo son accesibles a través del dominio .bit (http://www.dobit.me). Adicionalmente existe un mercado importante de compra/venta de dominios .bit con precios que van desde los 10.000 bitcoins para dominios como swissquote.bit o axabanque.bit hasta los 0.0001 bitcoins para dominios como bitcoinocean.bit o bitcoiplease.bit.

Namecoin proporciona por tanto una infraestructura de nombres de dominio que funciona completamente al margen de los DNS convencionales de Internet utilizando su blockchain para la resolución de los nombres. De esta forma no hay autoridades de registro, no hay servidores raíz, y no puede ser secuestrado, ni manipulado, ni sufrir los ataques habituales de los DNS de Internet.

Cuando un usuario registra un dominio .bit, el registro del mismo pasa a la cadena de bloques de Namecoin y queda almacenado y atribuido a la persona que lo haya dado de alta de forma temporal, con la posibilidad de ser renovado. Técnicamente hablando cada registro Namecoin consta de su clave criptográfica correspondiente (dirección) y un valor que puede tener hasta 520 bytes. De esta forma la clave f/midominio indica que un registro almacenado en el espacio de nombres f del DNS con el

nombre midominio se corresponde con el registro midominio.bit.

Un dominio se puede comprar en la actualidad con bitcoins o namecoins. En el caso de estos últimos, los nmc que han sido utilizados para comprar dominios se marcan como ya utilizados y se destruyen. Una vez que el dominio está registrado, la resolución del mismo se hace por consulta directa al blockchain de Namecoin. Con la especificación actual de Namecoin, cada dominio expira tras 36.000 bloques, el equivalente a unos 200 días, aunque siempre se pueden actualizar o renovar.

Como puede verse,Namecoin es un ejemplo de aplicación distribuida que utiliza la potencia del blockchain de Bitcoin para resolver el problema de los nombres de dominio de una forma distribuida, con un funcionamiento completamente autónomo y de forma segura. Es un ejemplo de aplicaciones para blockchain 2.0 que pueden funcionar con sus propios tokens a partir de la infraestructura desarrollada por Bitcoin.

Para finalizar, se realiza la comprobación de que Namecoin es realmente una dApp:

- Está escrita completamente y código abierto y es accesible a cualquier persona que quiera revisarla. Se puede acceder al mismo en la dirección https://github.com/namecoin.
- La dApp ha ido adaptando su código en función de los requerimientos y de los propietarios de los tokens. En la dirección anterior se pueden ver sucesivas revisiones de la dApp.
- Posee un token, el NMC, cuya evolución y cotización se puede seguir en lugares como Coinmarket: http://coinmarketcap.com/currencies/namecoin/
- Igualmente la generación de nuevos NMC se puede hacer mediante minería al igual que mediante webs de cambios como se puede ver en https://wiki.namecoin.info/index.php?title=How_to_get_Namecoins

Otras aplicaciones en blockchain 2.0

Se comentan a continuación otras aplicaciones descentralizadas destacables. Como se puede ver en la lista que se proporciona a continuación, la relación de aplicaciones es realmente extensa y muestra un ecosistema que ya es una realidad en torno al modelo de blockchain:

dApp	Descripción	URL
Eris Industries	Desarrollo de aplicaciones blockchain	erisindustries.com
Factom	Protocolo para permitir que las aplicaciones bitcoin 2.0 funcionen más rápido y de forma más económica en función del volumen de datos	www.factom.org
Storj	Almacenamiento descentralizado. Similar a Dropbox.	storj.io
La'Zooz	Sistema descentralizado de transporte, similar a Uber.	www.lazooz.org
Synereo	Red social de características similares a Facebook	www.synereo.com
Orisi	Pago por servicios de hosting sobre Oracle	orisi.org
Bitshares	Acceso universal a contratos inteligentes para la inclusión de nuevas características	www.bitshares.org
Ripple	Desarrollo de herramientas para instituciones financieras y sistemas de pago	www.ripple.com
Twister	Un Twitter descentralizado	twister.net.co
OpenBazaar	Comercio B2C. Una especie de Amazon utilizando moneda virtual y blockchain	openbazaar.org
Getgems	Una mezcla entre Whatsapp y Telegram con funciones adicionales relativas a envío de bitcoins y gems	getgems.org
Filament (Pinoccio)	Sensores para recolección de datos a nivel industrial	filament.com
Hawk	Almacenamiento cifrado de transferencias económicas	oblivm.com/hawk
SolarCoin	Valoración de la generación de electricidad vía energía solar	solarcoin.org
Augur	Apuestas y mercado de predicciones utilizando moneda propia	www.augur.net
D-cent	Herramienta para democracia directa por parte de los ciudadanos	tools.dcentproject.eu
Sidechain (blockstream)	Interoperabilidad entre diferentes blockchains	blockstream.com
Slock.it	Gestión de apertura de puertas utilizando	

Slock.it	blockchain	slock.it
Digix	Plataforma financiera para el estándar del Oro	www.digix.io
Nxt	Desarrollo de aplicaciones	nxt.org
eMunie	Creación y desarrollo de criptomonedas	emunie.com
Dash	Transacciones instantáneas con criptomonedas	www.dash.org
IOTA	Internet de las cosas	www.iotatoken.com
IDNI	Inteligencia artificial basada en razonamiento y ontologías	www.idni.org
Waves	Creación de tokens y comercio descentralizado	ico.wavesplatform.com
Supernet	Plataforma de criptoservicios	www.supernet.org

3
Blockchain 3.0

¿Qué es?

En los capítulos anteriores se hablaba de blockchain 1.0 como un nuevo sistema eficaz y válido para el intercambio financiero sin intermediarios y de blockchain 2.0 como un nuevo sistema para el desarrollo de contratos inteligentes y el desarrollo de mercados con aplicaciones similares a las que tenemos en la actualidad en los mercados digitales pero utilizando la potencia del blockchain. En el caso del 3.0 el reto tiene que ver con el desarrollo de nuevas tecnologías basadas en la identidad, la libertad, la democracia y la contabilidad de activos de cualquier tipo. Blockchain 3.0 tratará de solucionar las restricciones que actualmente existen en los mercados a nivel local, regulatorio y de entornos macroeconómicos. Es decir, mientras que blockchain 2.0 está tratando de migrar aplicaciones del mundo digital utilizando la trazabilidad y posibilidades de contabilidad en mercados masivos, blockchain 3.0 va a tratar de cambiar el status quo establecido utilizando la potencia, la deslocalización y la ubiquidad que generan las tecnologías blockchain.

No se trata de reinventar aplicaciones de mercado ya existentes, se trata de cambiar el mercado y de generar nuevos modelos de contabilidad y trazabilidad sobre activos de cualquier tipo desconocidos hasta el momento. Si se puede hablar de blockchain 2.0 como una evolución, en el caso de blockchain 3.0 se debe hablar de revolución. Esta revolución está por llegar, es algo que se va a ir produciendo en los próximos años, pero cuyas bases se están asentando en la actualidad. Hará falta bastante trabajo adicional para tener estos sistemas transaccionales completamente listos y en funcionamiento, no se ha hecho más que empezar. Las herramientas están parcialmente preparadas pero aún hacen falta bastantes elementos que en la mayoría de los casos tienen que ver con la interfaz de los activos del mundo real o digital y con la capacidad de trazabilidad y contabilidad que posee blockchain. Adicionalmente existe un problema de conocimiento general sobre estas tecnologías que se irán introduciendo en los próximos años. Las empresas TIC que se tendrán que encargar de desarrollar la base tecnológica del blockchain 3.0 no están todavía preparadas completamente y las empresas y organizaciones que se beneficiarán de

la aplicación de las mismas están aún identificando las estrategias necesarias para ponerlo en marcha.

Las dApps de las que se ha hablado en el caso del 2.0 están sentando las bases de esta revolución, pero su impacto local no es suficiente para la dimensión que va a ir adquiriendo 3.0 a nivel global. Como se va a ver a continuación, blockchain 3.0 tiene que ver con la regulación, con el cambio de las bases del mundo actual y con la interfaz de la mayoría de los activos que se gestionan en la actualidad.

La base del funcionamiento de blockchain 3.0 serán las DAS, de las que se habló en el capítulo anterior. Serán entidades autónomas, con capacidad de autogestión y generación propia de ingresos, con capacidad de funcionamiento distribuido, aséptico y transnacional.

En las siguientes secciones se van a exponer ejemplos y modelos de negocio sobre los que ya hay proyectos en algunos casos para la puesta en marcha de infraestructuras blockchain 3.0. En otros casos se exponen desarrollos que no pasan de la formulación teórica, pero cuya utilidad y dimensión sentarán las bases de modelos de negocio y de funcionamientos inéditos hasta el momento. Las diferencias con blockchain 2.0 parecen obvias. Se trata de cambiar conceptos globales, formas de funcionamiento que se daban por hechas y que tienen problemas obvios de regulación, transparencia, eficacia y democratización. Conviene dejar claro que en la actualidad son proyectos, que sufrirán modificaciones y que seguramente habrá aspectos que experimenten cambios importantes en su planteamiento, pero de alguna forma estos proyectos van a marcar el camino de la evolución futura de un blockchain más globalizado, útil y asentado a nivel no sólo financiero (blockchain 1.0), ni de mercados (blockchain 2.0), sino global y afectando a todas las capas de las sociedad que tienen que ver con la contabilidad y trazabilidad de activos humanos y físicos.

Gobierno y blockchain

Las aplicaciones descentralizadas orientadas al gobierno y los ciudadanos es uno de los proyectos más ambiciosos de blockchain. La realización de sistemas transnacionales que permitan una auténtica gobernanza por parte de la ciudadanía sería posible con niveles de granularidad desconocidos hasta el momento. No se trata sólo de que los ciudadanos puedan votar las decisiones, que hasta cierto punto es posible hoy en día, se trata de implantar un dinamismo en la administración que no ha sido posible hasta la fecha. La inmediatez en la realización de acciones a través de smart contracts será posible mediante la utilización de técnicas asociadas a blockchain 3.0 y posiblemente combinando otras asociadas a IoT y BigData. De esta manera las necesidades individuales por personas o familias podrán ser modeladas. Las organizaciones ciudadanas podrían optar por mejores o peores servicios en función de sus necesidades o podrían elegir simplemente pagar algo más por tener servicios algo mejores en ciertas áreas. Por ejemplo, un conjunto de ciudadanos podría decidir tener un mejor servicio escolar y pagar por ello. De forma automática se asignaría un incremento en sus impuestos que automáticamente repercutiría, vía smart contracts, en la calidad de los servicios recibidos a través de una asignación presupuestaria mayor con un objetivo concreto que sería acordado de antemano. No se precisaría intervención alguna de los organismos públicos, sería una acción inmediata sin la participación de intermediarios.

Se han propuesto tokens del tipo AccidentCoin con el cuál las personas involucradas en accidentes pagarían por la reparación de las vías de forma automática o RoadCoincon los que se pagarían impuestos de forma automática en función del uso de carreteras. Con este último token un activo del tipo carretera tendría la opción de autoadministrarse en función del uso que se haga de la misma para realizar sus propias reparaciones y para contratar servicios especializados de los disponibles en su smart contract en función del uso que se haga de la misma. Los usuarios en posesión de tokens de esta carretera en concreto podrían opinar con sistemas PoS (Proof of Stake) sobre la necesidad de reformar los smart contract asociados a la gobernabilidad de dicha carretera y sus

prioridades para las reparaciones o para la introducción de servicios adicionales. Mientras no hubiera nuevas opiniones sobre esos smart contracts el activo carretera tomaría sus propias decisiones en función de los Roadcoins que fuera acumulando y que la habilitarían para tomar decisiones sobre los servicios que pueda ir introduciendo y los trabajos que pueda ir contratando en función del presupuesto disponible por la circulación que se hace sobre la misma. Cualquier vehículo circulando por esa carretera contribuiría al mantenimiento de la misma, pero a la vez, conforme fuera contribuyendo tendría mayor voz para opinar sobre la gestión de los activos de la misma.

Se trata de ejemplos que generarían un mundo más equilibrado, democrático y sin la necesidad de intervención de terceras partes. Es un sistema de autoregulación individual de activos que complementa las teorías de Big Data e IoT en el contexto de las Smart Cities.

La relación de blockchain con Big Data es otro aspecto muy interesante para futuras aplicaciones. Hay que considerar que las tecnologías asociadas a Big Data tienen un carácter predictivo, pero carecen de mecanismos que permitan la toma de decisiones de forma en función de los resultados obtenidos. Es decir, Big Data informa, no toma decisiones en función de los datos extraídos. En un mundo que va a estar definido por la abundancia de datos y la incapacidad probable del ser humano para tomar decisiones en función de los mismos, o las mejores decisiones, con respecto a la incidencia de esos datos, blockchain puede ser la respuesta para que los datos sean capaces de gobernar a los propios datos. Es decir, blockchain se constituye como un sistema preparado para ejecutar acciones a partir de datos obtenidos por otras infraestructuras como es el caso de los desarrollos en torno a Big Data.

Problemas globales

Otro de los aspectos para los que ha sido propuesta la nueva generación de blockchain tiene que ver con la resolución de forma consensuada, democrática y sin intermediarios de los problemas globales. Un problema global en la actualidad es el hambre.

El problema que existe en la actualidad con cualquier tipo de donación que se pueda hacer para contribuir a solucionar problemas como puede ser el del hambre son los intermediarios y la seguridad de que los fondos depositados se utilicen para lo que realmente se quieren utilizar. Un ejemplo de estas nuevas formas de solucionar problemas en Sean Outpost (www.seanoutpost.com) un sistema para facilitar comida a personas con necesidad radicado en Pensacola, Florida, a cuya dirección Bitcoin se pueden enviar donativos desde cualquier parte del mundo para contribuir a la iniciativa. Los donativos se envían directamente a su dirección Bitcoin desde cualquier parte del mundo, sin intermediarios. Es decir, los fondos llegan directamente a la organización encargada de su ejecución. En la actualidad Sean Outpost ha servido ya más de 167.000 menús utilizando este sistema.

Portada de Sean´s Outpost, con la cuenta de Bitcoin de donaciones y más de 167.000 menús ya servidos por las donaciones

El ejemplo de Sean Outpost es sólo una pequeña muestra de lo que se podría hacer a nivel mundial con la gestión de donativos y su repercusión utilizando sistemas fiables basados en blockchain. La puesta en marcha de una moneda del tipo HungerCoin podría permitir donaciones instantáneas desde cualquier parte del mundo que fueran directamente a los implicados y que permitiera el acceso selectivo a alimentos en función de la posesión de dicha moneda. Permitiría la colaboración entre iguales sin intermediarios y de una forma democrática ya que cualquier persona con necesidad podría reclamar donativos directamente a su cuenta de divisa digital que podría utilizar solamente para la obtención de alimentos.

El asunto de los desastres mundiales es otra área interesante donde se podría aplicar la filosofía de blockchain. Cuando ocurre un desastre mundial, la aparición de hashtags de Twitter asociados al mismo es casi inmediata para la petición de ayuda. Sin embargo la canalización de esta ayuda es siempre lenta y poco eficaz. La generación de monedas

ayuda es siempre lenta y poco eficaz. La generación de monedas temporales asociadas a eventos concretos o más allá, la generación de cuentas digitales sobre monedas que se ocupen de eventos concretos podría facilitar y acelerar la llegada de ayudas a nivel mundial a organismos preparados previamente para el suministro. Igual que se extiende un hashtag en Twitter, se podría extender una cuenta digital que permitiera una muy rápida recaudación de fondos que sólo se pudieran utilizar para una acción concreta. Se trataría de acciones automáticas realizadas a través de smart contracts. Es decir, cuando este tipo de contratos consideraran un evento como un problema global según los registro que se pueden hacer utilizando mercados predictivos, se pondrían en marcha de forma automática los mecanismos de recaudación y envío de fondos, la contratación de las entidades que tienen que proveerlos y el depósito de los mismos en los lugares que precisan de los mismos. Esto permitiría incluso la categorización de la importancia y urgencia de las ayudas de forma automatizada.

En definitiva, la utilización de smart contracts puede permitir en el futuro una distribución más automática, equitativa y rápida de las ayudas para solucionar problemas globales, ya sean permanentes o puntuales. No se trata sólo de hacer llegar las ayudas de una forma rápida y sin intermediarios, se trata de poner en marcha las mismas y distribuirlas de forma consensuada a través de mecanismos automatizados que pueden tener los smart contracts. Es una cuestión de rapidez y de eficacia y blockchain presenta mecanismos para cumplir ambas cosas de forma más optimizada a como se ha venido haciendo hasta ahora.

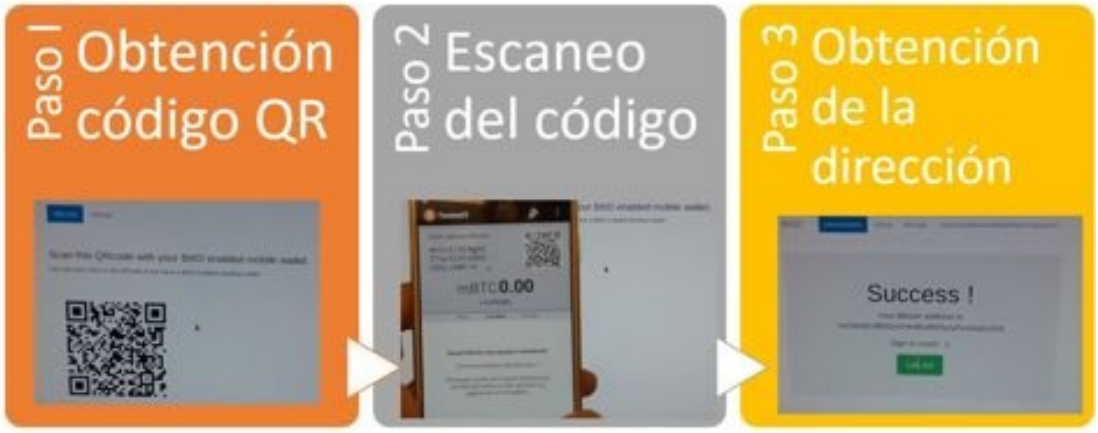
Identidades digitales

La identidad digital tanto de personas como de activos es otra de las innovadoras aplicaciones que puede tener blockchain en el futuro. No se trata sólo del poder de la identificación individual, que hoy en día se puede realizar por medio de la firma digital. Se trata de la reunión en una base de datos común, descentralizada y pública, de información y características sobre activos más allá de las personas.

Los servicios de identificación descentralizados que permite blockchain pueden aprovecharse de la posesión de las carteras digitales que permitirán mejorar la experiencia de usuario de forma anónima si se quiere, reforzar su seguridad y facilitar todo lo referente a pagos de forma instantánea. Existen ya proyectos de este tipo como son OneName, BitID o Bithandle que se comentan a continuación.

OneName (http://www.onename.com) es una aplicación distribuida desarrollada sobre Namecoin que permite identificar usuarios poseedores de carteras Bitcoin mediante un nombre en lugar de utilizar la dirección completa de Bitcoin que resulta imposible de recordar. Es una especia de sistema de resolución de nombres pero aplicado a personas en lugar de a dominios de Internet. Este servicio asociada una identidad completa blockchain a un nombre, permitiendo recibir mensajes de correo electrónico cifrados, realizar y recibir pagos fácilmente y se pretende que en el futuro sea una herramienta de login único a lugares web como se hace en la actualidad con las redes sociales.

BitID (http://bitid.bitcoin.blue) es otro sistema de identidad digital que permitirá en el futuro el login a cualquier aplicación web con una dirección Bitcoin. Hasta el momento se trata de un proyecto, pero en el futuro pretende unificar el login basándose en la dirección de la cartera Bitcoin de una manera sencilla, anónima y eficaz. El caso de Bithandle (http://www.hackathon.io/bithandle) es similar al de los anteriores al permitir la identificación de carteras digitales para hacer login con la dirección Bitcoin.



Utilización de BitID para la identificación de la cartera BitCoin

En cualquier caso los ejemplos anteriores provienen más de una generación anterior (blockchain 2.0) y no muestran realmente las verdaderas posibilidades que en el futuro pueden tener los sistemas de identificación digital con blockchain. El objetivo final debe ser la identificación de cualquier activo digital para dotarlo de personalidad propia y de capacidad, en caso necesario, de tomar decisiones de forma autónoma. El objetivo final es que cualquier activo, particularmente aquellos no humano, sean capaces de identificarse de manear única, puedan autoadministrarse y tengan capacidad para responder a demandas de otros activos.

Sería el ejemplo de una farola en una ciudad. La farola tendría una identidad única en el blockchain global de la ciudad y en función de su propio smart contract sería capaz de saber cuándo puede encenderse y cuándo no. Esta decisión se haría en función de los presupuestos que la entidad gubernamental le hubiera asignado y de mercados predictivos externos que serían en este caso los relacionados con las horas de luz. El propio smart contract de la farola tendría contemplado el cambio de la luz de la farola o de la pintura de la misma cada cierto número de años

luz de la farola o de la pintura de la misma cada cierto número de años. Sería este smart contract el que se encargaría de solicitar los servicios de otros smart contracts asociados a pintura o cambio de bombillas. En el momento que se hiciera un cambio de bombilla por ejemplo, el smart contract se encargaría de transferir los fondos a la empresa proveedora. Todas estas acciones se harían sin necesidad de intervención humana alguna. La farola se convierte de este modo en un activo digital identificado en un blockchain asociado a una smart city.

Sistemas de formación

En la actualidad ha habido un importante auge de plataformas de formación de diferentes tipos como es el ejemplo de los MOOCs. Esto ha generado una dispersión importante de objetivos por parte de los estudiantes por una parte y de posibilidades de verificación por otra. Nadie sabe muy bien cuántos cursos ha hecho una persona, en qué plataformas y qué valor tienen los mismos. Incluso los propios estudiantes que hacen estos cursos, unas veces en formato gratuito y otras veces a costa de su propio dinero, no tienen una referencia clara de dónde les va a llevar y cuáles son los objetivos finales. En muchos casos se hacen cursos porque están más o menos relacionados y pueden aportar más en el aspecto personal que en el profesional.

Una Learncoin podría solucionar en gran medida todo este problema permitiendo la financiación peer-to-peer de determinadas trayectorias educativas por parte de empresas u organismos interesados en tener personal con una determinada formación. En función de la superación de grados en cursos tradicionales o gestionados a través de la Learncoin, se podrían ir liberando a través de smart contracts nuevas learncoins que permitieran ir pagando niveles sucesivos hasta alcanzar las metas propuestas por las empresas o interesados. Esto crearía un mercado de oferta y demanda educativa contrastado, eficaz y basado en valores objetivos.

Un estudiante que quisiera alcanzar un determinado grado de formación en un área concreta podría acogerse al plan de formación que iría financiándose mediante learncoins y que al final del mismo podría abonar a la empresa que lo haya patrocinado con trabajo en torno al área, con la entrada en la empresa o simplemente abonando el importe con unos plazos establecidos. Los smart contracts sobre esta learncoin se encargarían se ir liberando recursos conforme se fueran cumpliendo objetivos en el programa formativo y por tanto garantizando el sentido de la formación y la preparación de candidatos de forma adecuada a las necesidades.

Esto además propiciaría la posibilidad de que cualquier persona, en

cualquier parte del mundo, pudiese acceder a este tipo de contratos e ir beneficiándose del mismo conforme fuera superando niveles. Estamos hablando en este caso de una democratización de las posibilidades de formación a nivel global.

No sería demasiada complicada la conexión con Mocos u otros cursos de formación ya establecidos aunque estuvieran fuera del circuito de Arrinconar. Simplemente se podría llegar a un acuerdo con ellos para la verificación y pago de los objetivos. En los casos donde no fuera posible, el propio smart contract podría ejecutar exámenes acompañados de identificación previa del usuario que certificara el cumplimiento de los grados en función de los cursos realizados.

Con el tiempo esta teórica Arrinconar (no existe a día de hoy) se convertiría en una base de datos casi universal donde se podría verificar de forma real y autenticada el número de cursos, grado de cumplimiento e incluso la mayor o menor calidad de los cursos realizados por cada estudiante en todo el mundo. Esto generaría, pensando en la conexión con Big Data, una fuente de “conocimiento sobre conocimiento” de un gran valor. Realmente se podría conocer con un grado de detalle bastante alto quiénes son los mejores especialistas en determinadas materias, qué personas están mejor preparadas para determinados trabajos y qué cursos son los que garantizan mejores trayectorias.

Esta última circunstancia generaría a su vez un gran interés y competencia entre profesionales por estar en la base de datos y por especializarse y progresar en determinadas áreas de forma que pudieran ser contratados por empresas para trabajos de especialización.

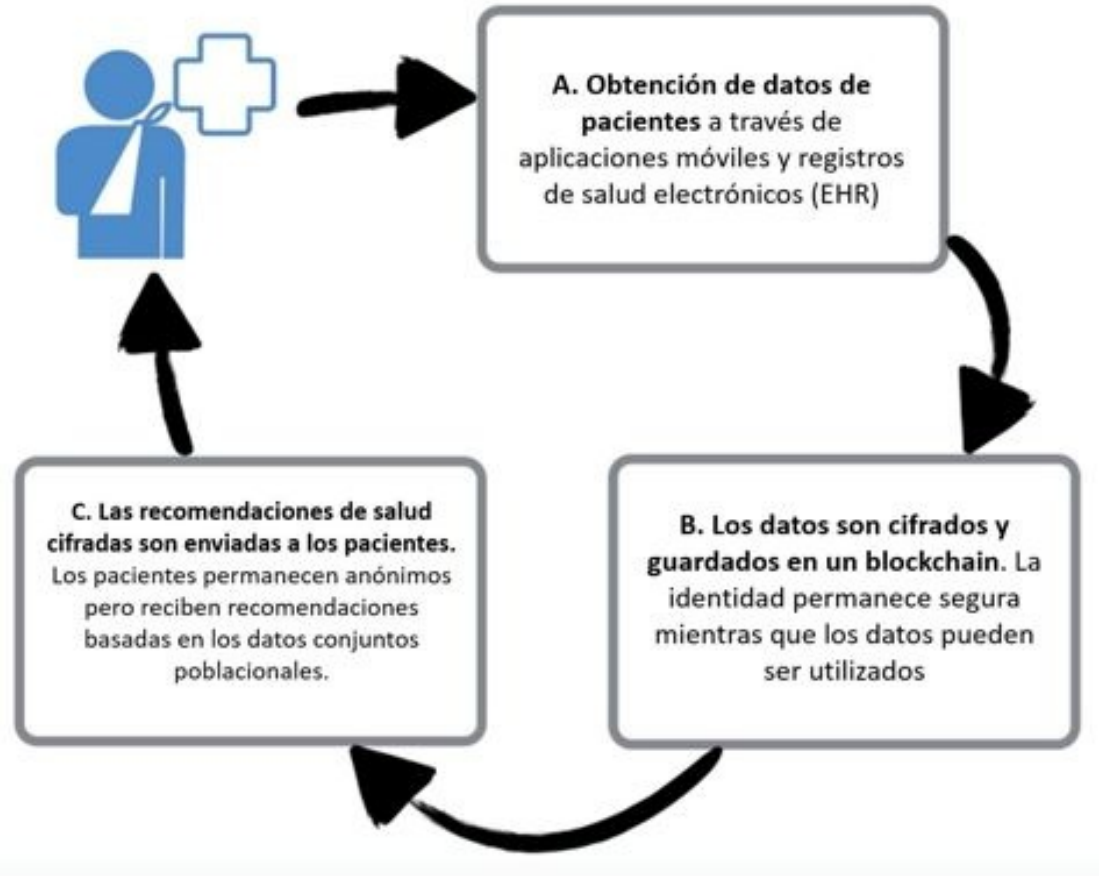
El experimento de Arrinconar es un buen ejemplo del poder de democratizan y universalidad de blockchain. El conocimiento quedaría abierto a nivel mundial y la democratizan del acceso a los trabajos así como del acceso a los trabajadores sería una realidad.

La salud y blockchain

Tras la lectura de los apartados anteriores, una teórica Helicoidal (no existente en la actualidad ni siquiera como proyecto) tendría una utilidad evidente. Esta utilidad iría más allá del control médico de un paciente y el acceso inmediato a sus datos por parte de cualquier institución.

La posibilidad del acceso a datos y tratamientos establecidos en la blockchain sanitaria permitiría realizar estudios imposibles hasta el momento. Hay que considerar que las entidades que quisieran experimentar con los datos de este blockchain sanitario tendrían acceso instantáneo y universal a los datos de millones de pacientes que serían totalmente anónimos a efectos de los datos extraídos, pero que permitirían la utilización de los mismos para estudios desde cualquier parte del mundo y por parte de cualquier institución. Estaríamos una vez más ante la democratizan del acceso a la información, en este caso médica.

Esta HealHealthcoinllar contratos inMOOCsentes que permitieran pagar con healthcoins a los poseedores de los datos utilizados en los estudios. El pago se haría a direcciones anónimas. Sólo el usuario sabría que ha sido pagado por la utilización de sus datos. Estas healthcoins se podrían utilizar posteriormente en entidades sanitarias para pagar tratamientos, análisis o cualquier otro tipo de procedimiento médico del que se pudiera beneficiar.



Aplicación del blockchain sanitario para recomendaciones basadas en datos conjuntos poblacionales

Los gobiernos podrían utilizar estas healthcoins para racionalizar el uso de los servicios sanitarios y controlar el gasto y uso que se hiciera de los mismos. El acceso a la sanidad privada para determinados tratamientos en función de localización, necesidades o saturación del servicio, podría hacerse de forma automática en función de la posesión por parte de los ciudadanos de healthcoins que les permitiera el acceso de forma automática en función de las circunstancias que se produjeran en cada momento. El gasto y el equilibrio de los servicios sanitarios se podría conseguir sin burocracia y de forma rápida y democrática una vez más.

De forma directa el uso de blockchain generaría para cada ciudadano un registro personal de salud que tendría múltiples aplicaciones tanto a nivel personal como a nivel de descendientes o de estudios más generalizados como se comentó con anterioridad. Cada paciente sería

dueño de su historial sanitario, que compartiría con quien quisiera de forma anónima o de forma verificada.

Lo expuesto anteriormente es sólo una parte de los servicios que una blockchain sanitaria podría proporcionar. Habría otros servicios a explorar y definir como pueden ser los seguros sanitarios, todo lo relativo a la genética y sus derivados como la farmacogenética, nutrigenética, etc, o servicios de competencia por la provisión de servicios privados sanitarios accesibles mediante esta healthcoin por cualquier paciente a nivel mundial.

Seguros

Los seguros es otra faceta que se podrá aprovechar de las capacidades de blockchain en los próximos años. Sin pérdida de generalidad se podría pensar en los seguros de coche.

El poseedor de un seguro de coche no tendría que pagar por él si no está utilizando el vehículo. Con el desarrollo de las tecnologías blockchain el seguro se pagaría sólo en el momento es que se fuera a hacer uso del vehículo. Este vehículo transmitiría de forma automática que se encuentra en funcionamiento. Esto permitirá también la posibilidad de escoger sobre el tipo de seguro y las coberturas en tiempo real en función de las necesidades. No tiene mucho sentido que un vehículo que vaya a estar estacionado un largo período de tiempo tenga que pagar por un seguro. Las compañías lo saben, pero hoy día es imposible certificar cuándo un coche está en movimiento y cuándo no lo está y registrar esta circunstancia de forma efectiva.

Otro aspecto importante que podrían resolver los smart contracts sería el caso de los accidentes. Los coches podrán llevar sensores capaces de evaluar automáticamente el daño recibido y elaborar partes instantáneos que puedan servir para realizar evaluaciones instantáneas, el coste de reparación de los mismos e incluso el sentido de la culpabilidad para las responsabilidades de pago. Esto podría generar partes automáticos de reparaciones para accidentes. Un vehículo involucrado en un siniestro podría estar siendo reparado a los pocos minutos de haber sufrido un accidente de circulación y el taller encargado de su reparación recibiría el dinero de la misma a los pocos minutos de haberse producido el accidente sin ni siquiera haber visto el vehículo.

Este ejemplo de seguros de vehículos podría ser extensible a prácticamente cualquiera de los aspectos contemplados por los seguros en la actualidad, como puede ser el caso de los seguros médicos, los del hogar, civiles, etc. Si existe un lugar donde contabilizar incidentes y automatizar acciones en función del resultado, los contratos inteligentes, configurados adecuadamente, serán capaces de discernir y automatizar

acciones que en la actualidad suponen meses de tramitación.

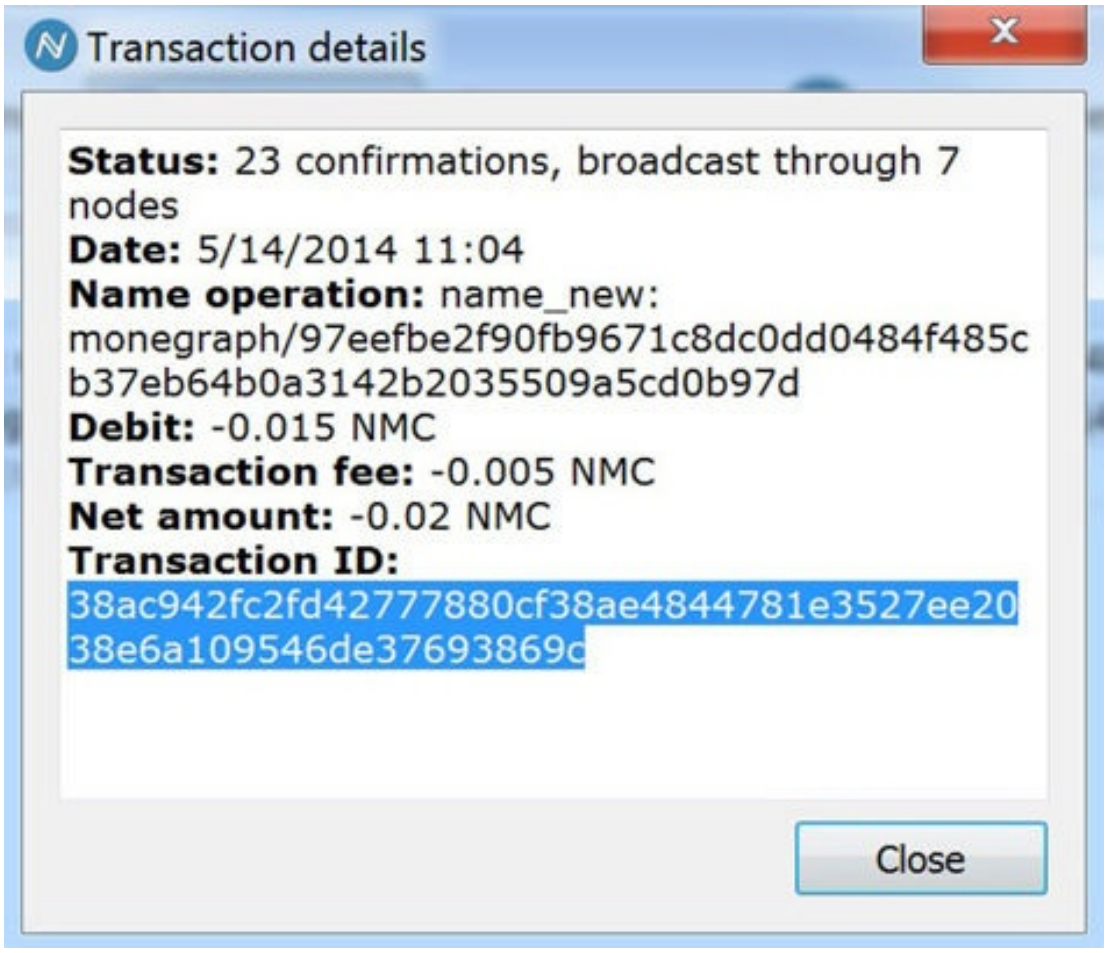
El ejemplo de Monegraph

Monegraph (http://www.monegraph.com) es un sistema ideado en un hackathon del New Musseum de Nueva York en 2014 por parte de Kevin McCoyyAnilDash. Su objetivo es proteger los derechos de autor de obras digitales y proporcionar ingresos para los creadores de obras de arte digitales, fotos de noticias, imágenes de productos e instantáneas en general. Las obras de arte digitales y las noticias se utilizan sin licencia comercial, mientras que las imágenes de productos y las instantáneas se pueden utilizar con licencia comercial.

Monegraph funciona sobre la blockchain de Bitcoin y de momento está restringido a obras en formato JPG, GIF y PNG de hasta 100MB, aunque en el futuro este límite será mayor y se extenderá al formato de vídeo.

La idea de Monegraph es que cualquier fotografía puede generar ingresos de forma distribuida, con independencia del medio en el que se use y sin permiso previo del autor de la misma porque el permiso ya ha sido concedido a través de blockchain. Monegraph sirve para dos cosas, en primer lugar se utiliza para verificar la identidad del autor original de una fotografía de forma permanente. A través del Monegraph Inspector (https://monegraph.com/inspect) se puede verificar el autor original de una obra. En segundo lugar sirve para obtener ingresos en bitcoins de forma directa por la utilización de una obra de arte con independencia del lugar donde se esté utilizando y sin necesidad de intermediarios que gestionen el pago de dichos derechos. En definitiva se trata de una plataforma de protección de los derechos sobre fotografías y de obtención de ingresos inmediatos por el uso de las mismas. Monegraph utiliza la blockchain de Bitcoin para gestionar la identidad de los poseedores de los derechos y para realizar los pagos, a través de Stripe (https://stripe.com), por el uso de las mismas. Las características de blockchain permiten fácilmente la compra/venta de estas fotografías entre particulares de forma instantánea. En el momento que se realiza la venta de una fotografía entre dos particulares, los ingresos asociados a esa fotografía que se están produciendo, pasan de forma automática e instantánea a la cuenta del nuevo propietario de la misma.

A nivel más tecnológico, Monegraph en una dApp de nivel 3, que utiliza Namecoin para la identificación de los activos y Twitter para su direccionamiento utilizando el sistema de nombres definido por Namecoin. Cuando un autor quiere registrar una fotografía lo hace a través de la API de Twitter y registra el tweet que genera a través de Namecoin obteniendo un bloque único que da de alta en el blockchain de Bitcoin utilizando Monegraph. Una vez que ha realizado dicha acción, la autoría de la obra queda registrada y se puede comenzar a explotar comercialmente. A nivel de utilización posterior del trabajo existen ya plugins en el mercado, como en el caso de Wordpress (https://es.wordpress.org/plugins/monegraph) que permiten la integración directa de obras digitales con licencias Monegraph en cualquier lugar web.



Detalles de una operación con Monegraph

Monegraph ha demostrado durante estos dos años de existencia cómo se pueden utilizar las propiedades del blockchain para comprar, vender y autorizar el uso de obras de arte digitales y cómo es posible establecer un mercado de derechos de uso distribuido y global que pueda beneficiar a los autores, pero que sea lo suficientemente flexible como para permitir la difusión masiva de estas obras y su utilización de una forma global, democrática y económica.

4
La tecnología detrás de blockchain

Conceptos básicos

Si ha llegado a esta página leyendo las secciones anteriores le habrá quedado claro el impacto cual será el impacto que una tecnología como blockchain tendrá en nuestras vidas en los próximos años. Pero la pregunta que puede estar haciéndose ahora es ¿cómo funciona Blockchain? La respuesta, aunque puede parecer lo contrario, es tremendamente sencilla, ya que la tecnología detrás de blockchain no es nueva, de hecho lo realmente disruptivo de Blockchain desde el punto de vista tecnológico es la forma en la que se han combinado distintas tecnologías ya existentes, como son las redes *peer-to-peer* o la encriptación de clave pública.

Para explicar cómo funciona Blockchain, antes tenemos que ver unos cuentos conceptos básicos que son la base sobre la que se construyen Blockchain:

- Red *peer-to-peer*. Una red Blockchain está formada por nodos que se comunican con un esquema descentralizado, en el que no existe un elemento orquestador. Este tipo de redes descentralizadas se conocen como redes *peer-to-peer*, porque los nodos se comunican de manera independiente con otros nodos que descubren en la red. La principal ventaja de las redes *peer-to-peer* es que son más sólidas frente a posibles contingencias, ya que los nodos funcionan de manera totalmente independientes.

- Encriptación de clave pública. Se utiliza este tipo de encriptación con dos propósitos en una red blockchain. El primero es que las direcciones que se utilizan para realizar las transacciones, es decir, las direcciones de emisor y receptor de una transacción, son en realidad una simplificación de la clave pública, de tal forma, que la clave pública realizan la función que la dirección IP tiene en la comunicación en Internet. Cualquier elemento que necesite realizar una transacción en una red blockchain necesita un par clave pública/clave privada para poder enviar y/o recibir transacciones. El otro propósito de emplear la encriptación de clave pública es que

todas las transacciones van firmadas digitalmente por el emisor, para garantizar la autoría de la transacción.

- Algoritmo de consenso. El principal problema de las redes descentralizadas es mantener la integridad de la información durante el proceso de actualización de la información que gestionan. Una de las soluciones más populares es la utilización de un algoritmo de consenso que todos los nodos de la red siguen para decidir qué nodo es el elegido para actualizar la información. En las redes blockchain se utiliza la prueba de trabajo POW (Proof of Work), en la que todos los nodos trabajan para resolver un reto, el primero que lo haga lo anuncia en la red para que el resto de nodos conozcan quién es el ganador y por tanto el nodo que podrá modificar la información.

- Los mineros. No todos los nodos de una red blockchain participan en resolver el reto de la prueba de trabajo, aquellos nodos que sí participan se conocen como "*mineros*" ya que el trabajo que realizan estos nodos se asemeja al trabajo de un minero, que debe trabajar para encontrar un metal precioso. En las redes blockchain, cada vez que un minero consigue resolver el reto recibe una recompensa por su esfuerzo, ya que al ser redes descentralizadas es la propia red la que debe pagar de alguna forma a los nodos para que estos trabajen para la red.

- Transacción. Es la operación básica en una red blockchain, mediante al cual una dirección de la red envía un mensaje a otra dirección de la red. En el caso de blockchains de monedas, las transacciones se corresponden con cantidades que un usuario o máquina, transfiere a otro usuario o máquina.

- Bloque. Se trata de un conjunto de transacciones que los mineros agrupan para poder resolver el reto. Los mineros intentan genera un bloque con una frecuencia fija y que varía según el tipo de Blockchain. Lo importante es que aquel minero que consiga el reto, además de obtener una recompensa por ser el ganador, incluirá el nuevo bloque generado, en la cadena de bloques y en este punto

comienzan de nuevo a minar el siguiente bloque.

Un ejemplo

Con un sencillo ejemplo vamos a ver cómo funciona la tecnología blockchain. Para el ejemplo vamos a suponer que Alice desea enviar a Bob una entrada de cine que acaba de comprar, para invitarle a ver una película. Supongamos que tanto Alice como Bob utiliza de manera asidua nuestra red blockchain TicketCoin. De hecho ambos dispones de una billetera digital que les permite operar con TicketCoin. Como ambos son amigos, tienen registradas en sus billeteras de TicketCoin la dirección del otro. Es decir Alice conoce la dirección pública de Bob y Bob conoce la dirección pública de Alice, ya que si no conocen la dirección del otro, nunca podrán realizar transacciones dentro de nuestra red blockchain.

Alice construye la siguiente transacción en su billetera electrónica y la envía a un nodo de TicketCoin

TxID Origen:	0x3d93fe329002
Origen	PubDir Alice
Clave pública de la firma	Clave pública de Alice
Firma	Contenido firmado
Destino	PubDir Bob
CodTicket	<Código entrada de cine>
Info	"Te invito a ver StarWars el próximo sábado a las 17:00 en los cines del centro comercial"

TxID Origen es el identificador de la transacción anterior en la que alguien envió el código de entrada a Alice, por ejemplo, la transacción que la plataforma de venta de entradas envió a Alice con el código de la entrada comprada. La Transacción de Alice tiene un ID que se construye mediante una función hash con el contenido de la transacción y da como resultado una cadena hexadecimal que identifica de manera inequívoca a esta transacción.

Transacción de Alice → Función(hash) → 0x43938d3a12ff

Transacción de Alice → Función(hash) → 0x43938d3a12ff

El TxID de la transacción de Alice es 0x43938d3a12ff. El identificador de una transacción no se almacena en la propia transacción, al ser la salida de una función, cuya entrada es el contenido de la transacción, es imposible que podamos incluir en la información de la transacción la cadena hash del contenido de dicha transacción.

El nodo recibe la transacción de Alice y lo primero que hace es comprobar que la transacción está bien formada. El segundo paso es comprobar la validez de la transacción, en este caso, el nodo debe contrastar con su copia local de blockchain que Alice es la última propietaria del código < Código entrada de cine>, busca las últimas transacciones cuyo destinatario sea Alice y que tengan el código correspondiente a <Código entrada de cine>, en caso afirmativo, valida la transacción y la incluye en el bloque para minar. También envía la transacción validada al resto de nodos de la red TicketCoin, que realizan la misma operación para validar la transacción.

En este punto, la transacción estará validada por un número de nodos, pero aún no ha sido incluida dentro del blockchain, es decir no ha sido confirmada. Para que una transacción sea incluida en el blockchain, los mineros deben recibirla e incluirla en el bloque que están minando. En este punto Bob puede consultar en el blockchain que existe una transacción de Alice con un código de una entrada digital de cine, pero aún no ha sido confirmada en el blockchain, por lo tanto no puede ser utilizada.

Al cabo de unos minutos (la frecuencia de generación de los bloques es una parámetro propio de cada red blockchain) la transacción se incluye en un bloque minado y en ese momento pasa a formar parte de blockchain y podemos decir que se ha confirmado dicha transacción.

Ahora Bob si tiene la seguridad de que Alice le ha enviado el código de una entrada de cine. Llama a Alice para darle las gracias y confirmarle que estará en el cine a la hora convenida.

El sábado siguiente, Alice y Bob están en la entrada del cine tal como

dice la información de la entrada. Para validar la entrada solo deben enviar una transacción con el código de entrada a la dirección blockchain que ven en un QR en la cola del cine. Bob abre la billetera electrónica de su smartphone, captura el QR y envía la transacción:

TxID Origen:	0x43938d3a12ff
Origen	PubDir Bob
Clave pública de la firma	Clave pública de Bob
Firma	Contenido firmado
Destino	PubDir Cine
CodTicket	<Código entrada de cine>
Info	Validar el ticket

Transacción de Bob → Función(hash) → 0x00384fad3211

En la entrada del cine un empleado puede comprobar que Bob es el propietario de la entrada, porque en blockchain ha quedado confirmada la transacción 0x00384fad3211 y por tanto es irrefutable que era el propietario de dicha entrada.

Este es un ejemplo sencillo de una aplicación basada en blockchain, en el que los usuarios, Alice y Bob, no solo pueden comprar entradas, también regalarlas y entregarlas en la entrada del cine. Una de las ventajas más importantes de este sencillo ejemplo frente a la gestión actual de bienes digitales como las entradas de cine, es que con blockchain el cine puede validar quién es el propietario real del ticket, aunque esta sea duplicado, ya que solo existe una cadena de transacciones validadas desde el primer propietario de la entrada, en este caso el cine, hasta el último propietario que presenta el ticket en la entrada.

Encriptación asimétrica

Desde tiempo inmemorial la principal preocupación de las personas que tenían que enviar un mensaje importante a otra persona, era poder garantizar que nadie consiguiera leer el contenido de dicho mensaje. Uno de los primeros métodos conocidos es el sistema César, que consiste en sustituir cada letra del mensaje por la letra situada X posiciones en el alfabeto.

HAY QUE VENCER A LOS GALOS DE ASTERIX

Modificamos 3 posiciones y obtenemos la siguiente cadena de texto.

KDB TXH YHQFHU D ORV JDORV GH DVWHULA

Ahora podríamos enviar el mensaje cifrado al destinatario, aunque en un paso anterior deberíamos haber comunicado al destinatario cómo puede descifrar el mensaje. El método César es lo que se conoce como sistema de encriptación simétrica, ya que se necesita conocer la clave tanto para encriptar como para desencriptar el mensaje. Pero el arte de la criptografía ha evolucionado bastante desde los tiempos de César y hoy en día los sistemas de criptografía simétrica son mucho más robustos que el método César, aunque comparten con éste una debilidad, que emisor y destinatario deben conocer la clave y aquí radica el principal problema al que se deben enfrentar los sistemas que utilizan criptografía simétrica. Cómo el emisor puede enviar la clave de encriptación al receptor con la seguridad suficiente para garantizar que nadie más tenga acceso a esa clave y por lo tanto al mensaje.

Para solucionar este problema se desarrollaron los métodos de encriptación asimétrica, en los que el emisor y el receptor no necesitan compartir la clave, de hecho cada uno tiene un par de claves que utilizan para encriptar y desencriptar. Este es el tipo de encriptación que se utiliza en Blockchain, no por su capacidad para encriptar mensajes, que no es estrictamente necesario, sino por la capacidad que tienen los sistemas de encriptación asimétrica para garantizar la autoría de un mensaje. Pero antes voy a explicar muy rápidamente cómo funciona la

encriptación asimétrica.

Supongamos que Marcos quiere enviar un mensaje cifrado a Pablo mediante un algoritmo de encriptación asimétrico,el primer paso es que Marcos y Pablo necesitan un par de claves conocidas como *Clave privada* y *Clave Pública*, no vamos a entrar en detalles técnicos sobre el par clave pública/clave privada, lo importante para el ejemplo es que la clave pública se genera desde la clave privada, es decir, existe una relación entre ambas, pero esta relación tiene una sola dirección, eso significa que con una clave privada podemos generar una clave pública, pero es imposible (desde el punto de vista temporal) generar la clave privada mediante su clave pública.

Marcos dispone de su par clave privada/clave pública.

Pablo también dispone de su propio par clave privada/clave pública.

Si Marcos quiere enviar un mensaje a Pablo, necesita conocer la clave pública de Pablo y la utilizará para encriptar el mensaje. En este momento el mensaje solo se puede desencriptar con la clave privada de Pablo, lo que garantiza que nadie que no tenga acceso a la clave privada de Pablo pueda acceder al contenido del mensaje.

La principal ventaja es que la clave para desencriptar el mensaje únicamente la conoce el remitente y por tanto, no es necesario compartir esa clave. El inconveniente, es que necesitamos conocer las claves públicas de todas aquellas personas a las que queramos enviar un mensaje encriptado.

A parte de poder enviar con seguridad un mensaje encriptado, los algoritmos de encriptación asimétrica tienen otra peculiaridad y es que permiten firmar un mensaje para garantizar que ha sido emitido por el emisor y que nadie ha podido modificar su contenido, ¿cómo se hace esto? De una manera sencilla, por ejemplo, supongamos que ahora nuestro amigo Pablo quiere enviar un mensaje a Marcos y no le importa que nadie más pueda ver el contenido, lo importante de este mensaje es que quien lo lea sepa que el emisor es Pablo.

Pablo utilizará su clave privada para encriptar el mensaje, en este caso para desencriptar el mensaje se necesita la clave pública de Pablo, es decir, cualquier persona que conozca la clave pública de Pablo podrá tener acceso al mensaje y tendrá la seguridad que solo Pablo ha podido encriptarlo, ya que solo con la clave pública de Pablo se puede desencriptar. Esto es lo que se conoce como firmar un mensaje, ya que lo importante aquí no es salvaguardar el acceso al contenido, sino disponer de un método que asegure que el mensaje ha sido emitido por quién realmente lo ha emitido y que nadie ha podido modificarlo.

Blockchain utiliza la encriptación asimétrica para firmar las transacciones, con el objetivo de garantizar la autoría de dicha transacción, de hecho, las direcciones blockchain son en realidad una cadena de caracteres que se genera a partir de la clave pública de cada usuario, mediante unas transformaciones HASH que convierte la clave pública en una cadena hexadecimal algo más pequeña de tamaño, con el objetivo de que se manejable.

Transacciones seguras

Las transacciones son el elemento base sobre el que funciona la tecnología blockchain por varias razones, pero la primera y principal es que los bloques de la cadena de bloques se generan con transacciones, por tanto podemos decir que la transacción es el ladrillo sobre el que se construye todo el sistema blockchain, la transacción es la unidad de información que se puede transmitir en una red blockchain.

Una transacción está compuesta por un conjunto de datos, depende de la particularidad propia de cada implementación de blockchain, el que las transacciones contengan más o menos información. Pero de manera general, las transacciones están formadas con los siguientes datos:

- Dirección pública del origen, necesaria para conocer quién ha generado la transacción.
- Dirección pública de destino, para blockchain pueda certificar la identidad del destinatario.
- Firma digital, con algunos de los campos de la transacción se genera una cadena de texto que se firma digitalmente con la clave privada del remitente, de esta forma, solo con la clave pública del remitente se podrá desencriptar el texto y por tanto se podrá confirmar que el remitente de la transacción es realmente el que ha generado dicha transacción, ya que únicamente él ha podido firmar el texto.
- Dato de la transacción, es el dato que queremos dejar almacenado en el blockchain, en el caso de un blockchain de monedas, sería la cantidad de moneda que se desea transferir.
- ID transacción origen, cualquier transacción necesita un ID de una transacción de origen, de tal forma que todas las transacciones tienen un padre y pueden tener varios hijos. Este campo es importante, porque sin él, blockchain no podría verificar la validez de las transacciones.

Existe otro dato que no forma parte de la transacción, pero que es un elemento clave para que el sistema sea consistente, el ID de la

transacción, en la lista anterior he comentado que uno de los campos que forman una transacción es el *ID transacción de origen*, pero ¿cómo sabemos el ID de una transacción? La respuesta es que el ID de una transacción es un identificador único que se genera con la información que contiene la transacción, es decir, necesitamos conocer el contenido de una transacción para poder calcular su ID. La razón de no almacenar el ID en la propia transacción, es que para validar la transacción debemos calcular su ID de todas formas y en el caso de que alguien modificase la transacción, como se ha modificado el contenido, también se estaría modificando el ID.

Un ejemplo de lo que podríamos ver en un bloque de blockchain sería algo parecido a esto:

	TxID Origen	TxID
0	0xAAAA	0xBCDA
1	0xBCDA	0xDHF3
2	0xBBBB	0x6DF4
3	0xDHF3	0xA2B3
4	0x6DF4	0xE3E1
5	0xE3E1 / 0xA2B3	0xAB34

Al estar las transacciones encadenadas, se puede realizar una trazabilidad de las mismas y esta es una característica esencial para el funcionamiento de Blockchain, la capacidad de poder trazar cualquier transacción para averiguar quién y cuándo se generó la transacción, de esta forma, es fácil asociar una transacción con la persona o máquina, que posea el par de claves pública/privada que firmó la transacción y en el caso de que dicha transacción se utilice para transferir un bien digital o una moneda digital, el sistema puede verificar la posesión del bien digital o el saldo actual que tiene el propietario que desea realizar la transacción.

Las transacciones son la base de la tecnología blockchain, ya que gracias a la firma digital y a la relación padre/hijo que existe entre todas las transacciones, se puede confiar en el sistema gracias a que todas las nuevas transacciones son validadas contra el Blockchain.

Una red descentralizada

Para garantizar la total autonomía e independencia de un sistema, una buena estrategia es construirlo de manera que no exista un elemento central u orquestador, es decir, el sistema funciona gracias a que todos sus elementos trabajan de manera coordinada, sin que exista un maestro que dirija la orquesta, en un modelo descentralizado, en el que los elementos interactúan con el resto de manera a como lo hace un grupo de peces nadando, en el que no existe un jefe, sino que el grupo se mueve por las pequeñas interacciones que tienen todos los peces con el grupo que nada más cerca de él. Los modelos descentralizados presentan algunas ventajas e inconvenientes frente a los modelos centralizados.

La principal ventaja de un modelo descentralizado es que tiene un mayor grado de resiliencia, ya que se reducen los puntos de fallo único. Tenemos que pensar en los modelos descentralizados como un conjunto de bailarines que ejecutan una coreografía de manera coordinada, si alguno de los bailarines comente un fallo o se cae, el resto puede continuar el baile, aunque el fallo afecte por proximidad a aquellos bailarines que estén cerca, el resultado es que la mayor parte del conjunto sigue bailando.

Blockchain implementa una solución de nodos trabajando en un modelo descentralizado, en el que no existe un nodo maestro, sino que los nodos se conectan entre sí formando una red *peer-to-peer* de nodos, a través de los cuales, la información circula por toda la red. Otra ventaja de los modelos descentralizados es que al no existir un nodo central, nadie gestiona las autorizaciones para participar en la red y por tanto, cualquiera puede crear un nodo para participar en la red blockchain. Este es el caso de las redes Bitcoin o Ethereum, solo hay que instalar el software necesario para convertir un PC o un servidor en un nodo Bitcoin o un nodo Ethereum.

Pero todo no son ventajas en las redes descentralizadas, también tienen inconvenientes y no son precisamente pequeños. El principal inconveniente es que al no existir un nodo o nodos centrales, a la hora

de actualizar la información que maneja el sistema, podemos encontrarnos con problemas de consistencia e integridad de la información. Por tanto, es necesario disponer de un protocolo que permita actualizar los datos de manera segura en una red descentralizada.

Supongamos que tenemos una red descentralizadas de 100 nodos, que gestionan una base de datos de usuarios, para este ejemplo, las transacciones podrían ser las modificaciones sobre los registros de esta base de datos compartida entre los 100 nodos. El primer problema que podemos tener es que dos nodos cualquiera, intenten modificar el mismo registro de la base de datos, si no implementamos un sistema para coordinar las actualizaciones de este tipo, cada nodo actualizaría su base de datos en local y seguidamente propagaría dicha actualización a los nodos más cercanos, de tal forma que en un tiempo t determinado por la velocidad de propagación, se producirían un conflicto, ya que a un nodo X llegarían dos actualizaciones distintas del mismo registro, lo que provocaría una inconsistencia en los datos almacenados.

Otra ventaja de las redes descentralizadas es que es más fácil detectar problemas de manipulación no autorizada de los datos, ya que es fácil comparar los datos almacenados en distintos nodos para identificar aquellos que han podido ser manipulados. Supongamos que alguien entra de manera ilícita en uno de los nodos y modifica un dato, por ejemplo, el email de un usuario. Como esta información está almacenada en el resto de los nodos, es fácil detectar en qué nodo ha sido manipulada y podría ponerse dicho nodo en cuarentena y volver a sincronizar con los datos de la red. De hecho, un atacante tendría que modificar el 51% de los nodos de la red para hacer que el 49% restante se viera obligado a resincronizar sus datos con los datos modificados por el atacante.

La cadena de bloques

Blockchain o cadena de bloques es la solución que se desarrolló en Bitcoin para el problema de mantener una base de datos en una red descentralizada de nodos. Blockchain es una solución brillante para resolver un problema complejo, y es brillante por una razón, tiene una concepción tremendamente sencilla.

El principal problema en una red descentralizada es disponer de un protocolo que permita coordinar las modificaciones de la base de datos con la que se está trabajando, Blockchain propone lo siguiente. Todos los nodos mantienen su propia copia de blockchain, los usuarios generan transacciones que envían a los nodos para que éstos las propaguen por la red blockchain. Cuando un nodo recibe una transacción la almacena de manera temporal e intentará construir o genera un bloque de transacciones, a esto se le conoce como minar un bloque. En realidad se trata de resolver un reto y es el siguiente. Todos los nodos de la red deben resolver el mismo resto, en el caso de Bitcoin, se trata de encontrar una cadena Hash cuyo valor en binario esté por debajo de un número, lo que se significa que los nodos deben generar cadena Hash con un número determinado de ceros al principio.

Esta cadena HASH será el identificador o nombre del bloque y se forma con la siguiente información:

- ID del bloque anterior.
- Todas las transacciones almacenadas en la memoria temporal.
- Un número.

Esta información puede variar dependiendo de la implementación de Blockchain con la que estemos trabajando, pero de manera general, estos son los tres elementos básicos. El ID del bloque anterior es necesario para mantener la cadena de bloques, ya que dentro de la información del bloque debe ir el ID del bloque anterior y no solo eso, estamos diciendo con esto, que de cierta manera, el ID del bloque anterior condiciona el ID del bloque que estamos intentando minar. La información con todas las transacciones y el tercer campo es un número. Esta información la debemos pasar a una función Hash y comprobar

Esta información la debemos pasar a una función Hash y comprobar cuantos ceros hemos conseguido, seguramente ninguno, debemos repetir el proceso, pero el único dato que podemos modificar es el número, ya que el resto es la información útil del bloque.

Si repetimos el proceso, modificando el número, en un tiempo t, alguno de los nodos conseguirá una salida de la función Hash que cumpla con el reto de la cadena que empiece con un número de ceros X, por ejemplo:

0x00000000000000003a2a20c0a0e936509b1f2720e4a3a10720753fb69765705

Este es un ejemplo de hash de un bloque de Bitcoin.

El nodo que haya conseguido el reto obtiene un recompensa, en el caso de Bitcoins es de 25 bitcoins (esta cantidad va decreciendo con el tiempo y es la única forma de generar nuevos bitcoins) y la suma de los feeds de todas las transacciones que están en el bloque que se acaba de generar. Una vez que lo ha generado, actualiza su cadena de bloque y propaga el nuevo bloque en la red. El resto de nodos irán recibiendo el nuevo bloque, lo validarán y lo incluirán en su propio blockchain.

De esta forma, se garantiza que todos los nodos están trabajando con la misma información, ya que solo un nodo, el que haya conseguido el reto, es el nodo que está autorizado a actualizar la cadena de bloques añadiendo el nuevo bloque que ha generado. En el momento que un nodo anuncia que ha generado un bloque nuevo, el resto de nodos comienzan a minar un nuevo bloque, comprueban la lista de transacciones que tienen en sus memoria temporal, eliminando aquellas que estén incluidas en el bloque que acaba de ser generado e intentando minar un nuevo bloque con las transacciones nuevas y las que queden en la memoria temporal.

Cuando una transacción llega a un nodo, lo primero que hace el nodo es validar la transacción, realizando ciertos checks, como son la firma digital o el saldo (en caso de que estemos hablando de blockchains para monedas digitales). La transacción está en estado validado, pero hasta que no forma parte de un bloque minado, no se puede decir que la

transacción esté confirmada.

Lo interesante de blockchain, es que la información queda almacenada en una cadena de bloques, los cuales no pueden modificarse, ya que cualquier modificación que se hiciese en un bloque alteraría la información del bloque y en consecuencia, modificaría su identificador o nombre, lo que supondría un problema ya que el bloque hijo estaría apuntando a un bloque que no existe. Al igual que ocurre con las transacciones, el identificador del bloque no se almacenan en ningún sitio, se debe calcular con al información del bloque y solo el hijo del bloque tienen almacenado el identificador de sus padre. Cualquier modificación en los datos necesarios para formar el identificador rompería la cadena.

La seguridad de Blockchain

Blockchain es una solución bastante segura y lo demuestra el hecho de que Bitcoin, a día de hoy, no ha presentado ningún problema grave de seguridad, que ponga en riesgo el sistema. Los problemas de seguridad relacionados con Bitcoin no tienen relación con el protocolo en sí, sino más bien, son problemas relacionados con el robo de claves.

La seguridad de una solución blockchain se basa en:

- Permite disponer de un histórico de transacciones con la garantía de que no se pueden modificar.
- La firma electrónica de cada transacción garantiza la autoría de las transacciones, con lo que es fácil identificar a los remitentes, en el caso de que podamos asociar firmas a personas.
- Todos los nodos disponen de su propia copia de la cadena de bloques, cualquier modificación de un bloque se puede detectar fácilmente, solo hay que comparar el bloque o la transacción de la que tenemos dudas con la copia que está en cualquiera de los otros nodos de la red.
- Tanto el ID de las transacciones como el de los bloques se generan mediante funciones hash y ambos se utilizan de manera tanto transacciones como bloques almacenan el ID de su padre.
- Cualquier modificación del contenido de una transacción o un bloque genera hijos huérfanos, rompiendo la cadena de bloques o de transacciones.
- Las transacciones tienen un emisor y uno o varios receptores, que si identifican con una clave pública, la cual está asociada a una clave privada, que es única, lo que garantiza de manera inequívoca al autor y destinatarios de una transacción.
- Un atacante debería coordinar una ataque al 51% de los nodos de una red para conseguir alterar con éxito un bloque. Por tanto, las redes blockchain son más seguras cuantos más nodos la formen.

5
Desarrollos para blockchain 2.0

Hyperledger Project y R3

En el último año la tecnología blockchain ha saltado a la primera plana de las noticias tecnológicas gracias a los informes de los principales analistas del sector, que identifican a blockchain como una de las tecnologías con más futuro en los próximos años.

Es curioso que una tecnología como ésta que está funcionando desde el 2009 gracias a Bitcoin, no se le ha tomado demasiado en serio hasta el año pasado. Lo interesante es que muchas grandes compañías se están interesando por las posibilidades de aplicación de blockchain en sus negocios y a diferencia de otros casos en los que la tecnología surge como respuesta a una demanda del público, en el caso de blockchain están naciendo muchas iniciativas aunque aún el gran público sigue únicamente relacionando blockchain a bitcoin.

Existe una iniciativa muy interesante llamada Hyperledger Project (www.hyperledger.org) que pretende establecer una serie de estándares para que la industria pueda adoptar soluciones basadas en blockchain. Esta iniciativa está liderada por compañías de la talla de IBM, Accenture, Intel, Hitachi, Fujitsu, J.P.Morgan, Cisco o VMWare entre otras muchas. Es un proyecto que acaba de comenzar y que seguro tendrá mucho que decir en el futuro, sobre todo por el peso de las compañías involucradas en el proyecto.

De todos los sectores económicos que muestran un interés real en explorar las posibilidades de Blockchain, la banca es el grupo que mayor interés está mostrando por conocer cómo puede una tecnología como Blockchain ayudarles a mejorar parte de sus procesos de negocio. De hecho resulta tremendamente paradójico que Bitcoin surgiera como una demostración real, de que un sistema financiero alternativo al tradicional, era posible. De hecho en muchos medios se identifica a Bitcoin como un auténtico killer para el sector bancario y en cambio, es el sector bancario el que mayor interés y recursos está dedicando para explorar las posibilidades de aprovechar Blockchain.

De todas las iniciativas, el consorcio R3 es una de las más

importantes, ya que agrupa a unos 40 de los principales bancos del mundo. El objetivo de este consorcio es explorar cómo Blockchain puede ayudar a mejorar algunos de los procesos tradicionales de la banca. De hecho, R3 no está interesado en el concepto de moneda criptográfica, ya que este interés iría en contra claramente de la base de su propio negocio, las monedas nacionales.

El interés real de R3 con Blockchain es identificar nuevas oportunidades en la forman en la que se pueden realizar transacciones seguras. Ya que para el sector bancario, es crucial poder asegurar todas las transacciones que un banco realizan con el exterior, ya sean otros bancos o los usuarios del propio banco.

Blockchain permite implementar transacciones totalmente seguras, lo que puede llevar al siguiente nivel, la relación entre los usuarios y su banco. Porque no se trata de que con blockchain un banco delegue toda la gestión de una cuenta al usuario, pero sí puede utilizar blockchain, por ejemplo, para conocer la reputación de un usuario que solicita un crédito, consultando su historial en una red blockchain por ejemplo.

Las aplicaciones son muchas y R3 tiene el objetivo de conseguir encontrar la forma de transformar la relación entre usuarios y bancos.

Ripple

Ripple no es un blockchain tal como se ha definido en este libro. Aunque comparte algunas características, como una base de datos compartida, una red de nodos y el concepto de transacción. La principal diferencia es que Ripple no utiliza mineros para generar nuevos bloques de la cadena de bloques.

En la tecnología Blockchain, los mineros tienen dos funciones básicas, la primera es que son los encargados de dotar de capacidad de procesamiento a la red, ya que son ellos los que aportar la potencia de computo necesaria para generar los nuevos bloques. Y por otro lado el hecho de que el proceso de generación de un nuevo bloque no sea un proceso determinista, es decir, no podemos predecir qué minero será el encargado de generar el nuevo bloque, hace que podamos confiar en la red, ya que es difícil manipular la información, por el famoso 51%.

Los mineros juegan un papel fundamental para garantizar la confianza en una red blockchain. Bien, pues Ripple sencillamente no utiliza mineros. De hecho su proceso de consenso se basa en la confianza que los nodos tienen sobre otros nodos. Esta relación de confianza evita la necesidad de tener que emplear mineros.

¿Cómo funciona Ripple? Básicamente de la misma manera que lo hace la tecnología blockchain. Un cliente genera una transacción y la envía a un nodo de la red Ripple, este nodo verifica la transacción y la incluye en una lista de transacciones candidatas, y la reenvía al resto de nodos de la red. Pasado un tiempo, la transacción habrá sido recibida por la mayoría de los nodos de la red.

Al igual que Blockchain, Ripple utiliza un algoritmo de consenso para decidir qué transacciones formarán parte del ledger compartido. El algoritmo de consenso de Ripple se basa en que un nodo pregunta a una lista de nodos en los que confía, sobre cada una de las transacciones candidatas. La lista de nodos de confianza o UNL (Unique Node List) devolverá una respuesta sobre si han validado la transacción, cuando el nodo recibe un número de respuestas positivas, sobre el 80%,

la transacción se considera buena para formar parte de la actualización del ledger compartido.

Cuando se ha llegado a un consenso sobre el listado de transacciones que formarán parte de la nueva actualización del ledger. Cada nodo genera un hash de validación con la información de las nuevas transacciones y propaga este hash al resto de los nodos. Cada nodo compara el hash que ha generado con los hash que ha recibido. Cuando un hash alcanza un consenso de más del 80% de los nodos. Se acepta este hash como el hash validado y todos los nodos aplican las transacciones a su propio ledger, con lo que se garantiza que todos los nodos están actualizando su ledger con el mismo conjunto de transacciones y por tanto, se garantiza que el estado final de todos los ledger será el mismo.

Como se puede ver, en Ripple no es necesario el uso de mineros, porque los nodos disponen de una relación de confianza establecida de manera manual, es el nodo el que decide confiar en otro nodo o no, al contrario de lo que ocurre con blockchain, en el que los nodos no deben confiar en sus vecinos, simplemente se decide quién será el siguiente en actualizar la cadena de bloques.

Una de las ventajas de Ripple es que el tiempo necesario para confirmar una transacción suele rondar los 2 o 3 segundos, lo que es muy interesante sobre todo para transacciones en tiempo real.

Ripple está teniendo una acogida muy prometedora en el sector bancario, ya que es una alternativa segura para las transacciones tanto internas dentro de una entidad, como aquellas transacciones que se realizan entre las entidades.

El problema del almacenamiento

Cualquier sistema de información debe cumplir con dos principios básicos, poder almacenar la información y tener la capacidad de procesarla. El almacenamiento y el procesamientos de la información son dos características que condicionan a la mayoría de los sistemas de información, de hecho diseñar y construir sistemas de información que optimicen tanto el almacenamiento como el procesamiento de la información es el reto al que se enfrentan cada día muchos ingenieros IT.

En una economía que nos obliga a optimizar los recursos disponibles y en la que gran parte del esfuerzo de construcción de nuevos sistemas se consumen en la optimización de las tareas necesarias para procesar la información, de pronto aparece una tecnología como Blockchain, en la que el foco no está puesto en optimizar los recursos, sino en asegurar la autoría de la información para garantizar la transacción de la información entre dos elementos.

Desde el punto de vista de un arquitecto IT, Blockchain puede ser una tecnología segura, pero hace uso de los recursos de una manera no demasiado óptima, ya que toda la información que se maneja dentro del sistema está replicada en todos los nodos de la red. Esto significa que si tenemos una red con 10.000 nodos y queremos realizar una transacción para enviar un dato a otra personas, por ejemplo, una cadena alfanumérica de 6 caracteres.

X83DF9

Sin contar con la información de la propia transacción, estaríamos almacenando 6bytes x 10.000 nodos, es decir, nuestros 6 sencillos caracteres estarían ocupando uno 58 Kbytes, es decir, la información estará ocupando 10.000 veces su tamaño, tantas veces como nodos tengamos en la red.

Si la tecnología Blockchain ha demostrado que funciona es por esta razón, porque todos los nodos almacenan toda la información, lo que hace resistente el sistema a muchos tipos de contingencias, como son los ataques de denegación de servicios. El problema es que estamos utilizando una gran cantidad de espacio de almacenamiento y desde el punto de vista de la optimización de los recursos es algo que chirría bastante y que si bien, Blockchain ha demostrado ser una tecnología útil para un sistema de transacciones monetarias, en las que la información que se transmite en un transacción es muy pequeña (la cantidad de moneda que se transfiere), y por tanto no es demasiado relevante este uso no optimizado del almacenamiento, en el caso de que queramos utilizar una red blockchain, para realizar transacciones de información que requieran un tamaño mayor, por ejemplo, 200KBytes de una imagen PNG, por ejemplo, se deben buscar alternativas para evitar que el tamaño de las propias transacciones termine saturando la red.

	Bytes	**10K nodos**	**1 Mill. Usuarios**
Código	6 Bytes	~58KB	~55GB
Imagen	200KB	~1,9GB	~1.862 TB
Documento	3MB	~29GB	~28.600 TB

Esta tabla muestra el tamaño medio necesario para gestionar las transacciones en una red con 10K nodos y un millón de usuarios. Como se puede ver, los números crecen de manera extraordinaria y en la tabla no se ha tenido en cuenta la cantidad de espacio necesaria para almacenar toda la cadena de bloques, ya que tendríamos que multiplicar a la última columna la longitud del histórico.

Para las nuevas redes blockchain, hay que plantear un nuevo esquema de almacenamiento, en el que por un lado se almacenen las transacciones en todos los nodos y por otro lado, se pueda almacenar la información de manera óptima. Por ejemplo, supongamos que deseamos enviar a Blockchain una transacción en la que queremos adjuntar un fichero de 200KBytes, ahora, dependiendo de la red blockchain que utilicemos, deberíamos dividir el fichero en porciones más pequeñas y enviar su contenido en distintas transacciones, las cuales se replicarían

en la red blockchain en cada uno de los nodos, una vez que dichas transacciones formasen parte de un bloque.

Una propuesta podría ser, disponer por un lado de transacciones clásicas en las que enviamos información a la red blockchain y de transacciones especiales, que no se replicasen en todos los nodos, solo en un número de ellos, lo suficientemente grande para garantizar que no se puede manipular la información. Una solución sería disponer de una segunda red blockchain, dependiente de la primera, pero que fuese más pequeña y especializada en almacenar ficheros, de esta forma, se reduciría la cantidad de espacio necesario para almacenar los ficheros. Construir redes blockchain de este forma, permitirá optimizar los recursos, ya que de no ser así el riesgo de este tipo de tecnología es que puede morir de éxito.

El problema del procesamiento

Si como se ha visto en el apartado anterior, el almacenamiento es un problema para el crecimiento de las redes blockchain, lo es más si cabe el procesamiento. El almacenamiento es infinitamente más barato que el procesamiento, por una sencilla razón, el coste de almacenar un byte es muy pequeño, ya que la tecnología de almacenamiento ha ido reduciendo su precio de manera progresiva. Cada vez hay más demanda para almacenar la información, lo que ha empujado a los fabricantes a una carrera para optimizar las soluciones y reducir el precio del bytes almacenado.

Al principio de los 80's el coste de un Gbytes era de unos 300K dólares, a día de hoy el coste del GB está sobre los 0,02 dólares. Es decir, el coste del almacenamiento se ha reducido tanto que no supone un problema de tipo económico para un proyecto. Es algo que por ahora no debe preocuparnos. El problema a acentúa en el otro recurso de cualquier sistema de información, el procesamiento. El coste de procesamiento de información se ha ido reduciendo con los años, la mala noticia, es que no lo ha hecho al mismo ritmo de que la reducción del almacenamiento, lo que ha provocado que exista una enorme diferencia entre el coste de almacenar información y el de procesarla.

El problema que se plantea es que una red blockchain procesa la información de manera redundada, es decir los nodos están intentando resolver el reto para poder generar el nuevo bloque. Este procesamiento de información les obliga a consumir ciclos de CPU y por tanto de energía y en esto se basa parte del planteamiento de blockchain, que no puedas obtener una recompensa sin haber gastado energía de procesamiento. De hecho en cada generación de un nuevo bloque, solo un minero tendrá éxito, lo que significa que el trabajo de procesamiento del resto de la red no ha servido para nada, es decir, toda la red de nodos que intenta minar un nuevo bloque han gastado energía para nada.

También hay que tener en cuentan, que en redes como Bitcoin, el procesamiento se utiliza para minar nuevos bloques, lo que sostiene por

así decirlo al propio sistema. Con la aparición de los Smart Contracts de Blockchain 2.0, además del procesamiento que necesitan los mineros para encontrar nuevos bloques, hay que añadir el procesamiento que necesita ser asignado a un Smart Contract para que puede ejecutarse. Porque al igual que ocurre con la información de una transacción, que se replica en todos los nodos, una vez forma parte de un bloque. Un Smart Contract se debe ejecutar en todos los nodos de la red, lo que supone un consumo extra de procesamiento, que se irá incrementando con el número de smart contracts que se almacenen en la red.

Otro reto importante para blockchain, es que debe optimizar el uso de los recursos de procesamiento, ya que debido a los problemas medioambientales a los que nos enfrentamos en el planeta y a que las personas estamos cada vez más concienciadas con el uso responsable de los recursos. El planteamiento de malgastar energía, sencillamente porque podemos hacerlo va en contra de la actual cultura medioambiental de la población y puede ser un verdadero obstáculo para que blockchain sea una tecnología aceptada por la sociedad.

Un solución, al igual que se propuso en el almacenamiento, podría ser emplear nodos especializados para ejecutar código dentro de una red blockchain, de esta forma, se podría minimizar la cantidad de energía que se desperdicia en el proceso, tanto de la generación de nuevos bloques, como en la ejecución de código dentro de la propia red.

Es condición necesaria para que Blockchain pueda llegar a convertirse en una tecnología de aplicación universal, buscar alternativas al problema del almacenamiento y el procesamiento. Blockchain debe seguir evolucionando para transformarse de un sistema seguro de transacciones para monedas virtuales, a una nueva forma de comunicarnos, tanto entre las personas, como entre las propias máquinas. Pero este hito necesita de una transformación de la arquitectura Blockchain, al igual que ocurrió en los albores de Internet, es necesario explorar las posibilidades que ofrece la tecnología para crear nuevas aplicaciones, evolucionando lo que tenemos para que se ajuste a lo que necesitamos.

Blockchain ha demostrado ser una tecnología lo suficientemente disruptiva para que haya llamado la atención de gran parte del sector IT. Tenemos dos opciones, pensar en cómo podemos crear nuevas aplicaciones para utilizar la tecnología blockchain en su estadio actual o lo que es más ambicioso y por tanto más prometedor, transformar Blockchain para que se ajuste a las necesidades que demanda el mercado.

Código dentro de blokchain

Cómo se ha descrito en la primera parte del libro, Blockchain sigue evolucionando desde el denominado Blockchain 1.0, que ha demostrado la solidez de esta tecnología, al ser el soporte de monedas virtuales como Bitcoin. El siguiente estadio de evolución es blockchain 2.0 y es en el que nos encontramos actualmente. Blockchain 2.0 ha ampliado las posibilidades de la versión anterior para conseguir, no solo ser una solución para monedas virtuales, sino una herramienta que ayude a transformar algunas de las actividades de nuestra vida digital. Estas nuevas posibilidades se han centrado en los denominados contratos inteligentes.

Los contratos inteligentes han abierto una nueva puerta para poder crear sistemas autónomos que nos liberen de ciertas tareas. Ya que mediante un contrato inteligente, podemos delegar ciertas operaciones, como pagos a terceros o reembolsos, a pequeñas aplicaciones que se encargan de gestionar de manera autónoma este tipo de operaciones.

Las dos iniciativas más populares de implementación de contratos inteligentes son Ethereum y Codius. De Ethereum se ha hablamos en secciones anteriores del libro, se trata de un blockchain desarrollado a partir del concepto de Bitcoin y que permite entre otras cosas poder generar monedas virtuales y ejecutar contratos inteligentes.

Un contrato inteligente para Ethereum es un trozo de código escrito en un lenguaje de programación como Serpent, LLL o Solidity. Una vez hemos escrito el código, lo debemos compilar para transformarlo en bytecode que se pueda ejecutar dentro de la máquina virtual de Ethereum. Este código se publica dentro de la red blockchain de Ethereum y se le asigna una dirección pública. Gracias a esta dirección pública, personas u otros contratos inteligentes, se pueden comunicar con él mediante transacciones. Es decir, una vez nuestro contrato está publicado en el blockchain de Ethereum podríamos realizar una transacción en la que el destinatario sea el contrato y a su vez, el contrato también puede realizar transacciones dentro de la red.

Ethereum dispone de una base de datos distribuida gracias a la tecnología blockchain desarrollada para bitcoin, ya que se ha basado en este planteamiento para desarrollar su propio blockchain, que tiene algunas características diferentes, por ejemplo, la generación de un bloque de la cadena es cada 12 segundos, frente a los 10 minutos que emplea Bitcoin. Aunque la capa de almacenamiento de transacciones es similar a la de Bitcoin, Ethereum ha tenido de desarrollar una solución para poder ejecutar los contratos inteligentes en una red descentralizada de nodos.

La solución de Ethereum ha sido, que en un bloque, no solo se almacenan transacciones, también se almacena el código del contrato y el estado de dicho contrato. No debemos olvidar que al fin y al cabo, los contratos no dejan de ser código que se ejecuta en un sistema y que puede estar en varios estados, dependiendo de cómo lo hayamos programado. Es importante que los bloques del blockchain almacenen el estado de ejecución de un contrato, de tal forma, que cada vez que un contrato se ejecuta, según la entrada que reciba, el minero debe almacenar el estado en el que ha quedado el contrato. Con esta información sobre el contrato, intentará construir un bloque y ganar el reto. Si lo consigue, el contrato y su estado actual quedarán almacenados en la cadena de bloques.

El problema de esta solución, es que el contrato se ejecuta en todos los nodos mineros, lo que supone un gasto considerable de energía asociada al consumo de CPU de los mineros. Ya que ahora el minero, no solo debe emplear su energía para mantener la cadena de bloques intentando minar bloques, sino que debe ejecutar el código de los contratos. Si como se ha planteado en el apartado anterior, uno de los retos que debe afrontar blockchain es transformar su forma de utilizar la capacidad de procesamiento disponible, el caso de las implementaciones para soportar la ejecución de código dentro de un blockchain no pueden basarse en un modelo en el que el mismo código se ejecuta en una gran cantidad de nodos de manera repetida.

De hecho, la otra iniciativa Codius, desarrollada inicialmente por Ripple ha abandonado el desarrollo y lo ha puesto en manos de la comunidad

ha abandonado el desarrollo y lo ha puesto en manos de la comunidad, para que pueda evolucionarlo. La realidad es que, aunque es necesario disponer de una forma para que blockchain pueda ejecutar código, el planteamiento de ejecución en paralela del mismo código presenta el inconveniente de malgastar un recurso muy preciado como es la CPU.

La comunidad debe plantear alternativas a este modelo de ejecución de código, en el que se optimice el uso de los recursos, por ejemplo, mediante nodos dedicados a la ejecución de código, que eviten que los mineros empleen CPU para ejecutar código. Estos nodos podrían almacenar el código en formato bytecode y estar leyendo de una blockchain de transacciones para ejecutar el código según las transacciones que reciba. El estado del código se puede enviar a la blockchain para que tanto los clientes, como el código almacenado en otros nodos pueda conocer el estado en el que se encuentra la ejecución.

Con estrategias del estilo *round-robin* los clientes o la misma red blockchain podría decidir qué servidor de ejecución ejecutará el siguiente estado de ejecución y comparar el estado generado por la ejecución del mismo código en varios nodos distintos.

El objetivo al fin y al cabo, es ir transformando el esquema de blockchain que conocemos ahora, por un esquema más robusto y que haga un uso más inteligente de los recursos disponibles.

El tamaño de la cadena

Una de las características que convierte a blockchain es una solución tremendamente sólidad es la capacidad para mantener un historial de todas las transacciones que se han realizado desde la puesta en marcha de la cadena de bloques. Esto permite por ejemplo, que en el blockchain de Bitcoin podamos consultar las transacciones desde 2009, que fue el año en el que se puso en marcha Bitcoin.

El disponer del historial de las transacciones es fundamental para construir una moneda virtual como bitcoin, ya que blockchain no almacena el saldo, sino que almacena todas las transacciones que se realizan y se reconstruye el saldo consultando las transacciones. Sin la cadena de bloques completa, no se puede conocer el saldo que tiene una dirección Bitcoin.

Ahora bien, el que tener el historial de todas las transacciones sea la base para soportar una moneda virtual, no significa que sea una ventaja para otro tipo de aplicaciones. Pensemos en una red blockchain para almacenar datos generados por dispositivos, por ejemplo, el consumo de una farola de la calle. El ayuntamiento podría tener conectadas todas las farolas y elementos urbanos que consuman electricidad, a un red blockchain para registrar el consumo y poder enviar comandos de operación a estos elementos, la cuestión es ¿sirve de algo tener almacenados los datos de más de un año? En una red blockchain cuyo base no sea una moneda virtual, no tendría mucho sentido tener un histórico completo de las transacciones, quizás un perido más reducido puede ser igual de útil para mantener la consistencia de las transacciones y evitaría malgastar una cantidad enorme de espacio de almacenamiento para datos. Una solución prodría ser realizar consolidaciones de las transacciones estableciendo de manera periódica un corte y consolidar hasta ese corte, para poder eliminar la información anterior al corte.

Otra opción para reducir el tamaño de la cadena de blocque podría ser plantear transacciones con un tiempo de vida establecido, de forma que

una vez finalizado este tiempo de vida, se podrían eliminar de la cadena de bloques. Aunque esta purga de transacciones debería hacerse de forma gradual, ya que por la forma en la que se construye la cadena de bloques, al modificar un bloque estamos modificando su contenido y en consecuencia estamos alterando el resultado de la función Hash que se aplica para identificar a un bloque y si alteramos un bloque, también debemos modificar el bloque hijo, porque el hijo tiene un puntero a su bloque padre y así seguiríamos modificando y recalculando los identificadores de cada bloque hasta llegar al último bloque.

Uno de los retos es conseguir reducir el tamaño de la cadena de bloques en aquellos aplicaciones en las que sea innecesario mantener un histórico total de transacciones, optando por soliciones como consolidaciones e históricos parciales.

El eslabón débil, la wallet

El punto fuerte de la tecnología blockchain es a su vez su punto más débil, se trata de las wallets o carteras electrónicas. La realidad es que utilizar el término wallet o cartera no ha sido demasiado afortunado, de hecho, este término genera demasiada confusión en el usuario, haciéndole pensar que por ejemplo BitCoin funciona de una forma que realmente no es correcta.

Pero antes de continuar ¿qué es realmente una wallet en la terminología Blockchain? Una wallet es un repositorio de software en el que se almacenan el par clave pública/privada. No se almacena nada más, esta es la razón de que genere confusión en muchos usuarios, ya que la mayoría piensa que en su wallet se almacenan las monedas virtuales, por ejemplo, los bitcoins y que sus bitcoins están completamente seguros porque los tiene guardado en un pendrive. La realidad es que en la wallet no se almacenan bitcoins, ni ningún otro tipo de moneda virtual basadas en Blockchain. La wallet se encarga de almacenar nuestras claves públicas/privadas y dependiendo de la wallet, algunas son capaces de generar transacciones.

¿Por qué la wallet es el eslabón más débil? La respuesta es sencilla. Todas las transacciones en blockchain van firmadas digitalmente y el destinatario de una transacción está asociado a una clave pública, solo la persona que tenga la posesión de la clave privada asociada a esa clave pública, podrá reclamar ser el destinatario de esa transacción. Por tanto, si alguien pierde su clave privada, no podrá firmar nuevas transacciones y en consecuencia no podrá reclamar ser el legítimo destinatario de una transacción.

Y perder la clave privada no es lo peor que nos puede ocurrir, es aún peor que alguien nos la robe, ya que en ese caso esta persona es la propietaria legítima de todas las transacciones que tengan como destinatario la clave pública que acaba de robar. El problema radica en que Blockchain no tiene el concepto de identidad asociado a personas o aplicaciones. El propietario de un bien digital es aquel que posea la clave privada que le permita presentarse como el destinatario de la

transacción.

De hecho, al no existir una relación directa entre la identidad del propietario y la posesión de la clave privada, permite que una wallet pueda gestionar cientos o miles de pares de claves pública/privada. Podríamos tener tantos pares como cuentas de email tenemos actualmente. De hecho es algo parecido a lo que ocurre con el email. Cuando alguien nos da su dirección de email, no tenemos forma de comprobar si es el auténtico propietario de ese email, ya que no existe un registro central en el que podamos verificar la autenticidad de un email. Algo similar ocurre con las wallets y los pares de claves pública/privadas.

Blockchain es una tecnología tan segura como el esfuerzo que hagamos para mantener segura nuestras claves privadas.

Más redes Blockchain

A día de hoy podemos encontrar diversas alternativas que implementan la tecnología Blockchain para crear redes de nodos. Pero todas estas redes se han planteados desde la premisa de construir una infraestructura IT, es decir, una red peer-to-peer de nodos, sobre la que se despliega una implementación de Blockchain, con más o menos características y que cubren una u otra necesidad. Este enfoque generalista es interesante en un estadio inicial como en el que nos encontramos. Hay que dotar de infraestructura base a las nuevas aplicaciones que se plantean desarrollar y es necesario que exista esta infraestructura base, porque sin ella, sería imposible que desarrolladores independientes pudieran crear nuevas aplicaciones.

El problema de tener redes generalistas, es que todas las aplicaciones que se desarrollen con una tecnología concreta, compartirán la misma red de nodos, lo que puede suponer un grave problema a medio o largo plazo. Por ejemplo, supongamos que creamos una nueva plataforma Blockchain la cual llamaremos Krypton (en honor a Superman), en un momento determinado alguien desarrolla una nueva aplicación para comprar/vender tickets de eventos, y los usuarios comienzan a utilizar Krypton como plataforma Blockchain para la compra y venta de entradas. Al mismo tiempo una compañía eléctrica crea una aplicación en Krypton para gestionar los contadores de la luz y el consumo de los aparatos eléctricos. Miles de aparatos comenzarán a realizar transacciones sobre nuestra red Krypton y terminarán impactando de manera negativa a la aplicación de compra venta de entradas.

Aunque el ejemplo puede parecer absurdo, la realidad es que es necesario no solo crear nuevas plataforma Blockchain, sino que es imprescindible que dichas plataforma puedan desplegar distintas redes menos generalistas y más especializadas. Por ejemplo, Krypton podría disponer de distintas redes como:

- Una red para aplicaciones de imágenes.
- Una red para Internet de las Cosas.

- Una red médica.
- Una red para aplicaciones académicas.

Al segmentar la especialización de las distintas redes, complicamos la arquitectura de la solución Blockchain, pero estamos garantizando que los recursos se utilizan de una manera más inteligente y evitamos problemas con la escalabilidad de la plataforma.

Ser los propietarios de nuestra información

Una de las ideas más disruptivas que está detrás de la tecnología blockchain, es el cambio radical que se produce a la hora de gestionar nuestra propia información. Tradicionalmente los sistemas de información se construyen desde una perspectiva centralizada, en la que el sistema recoge, almacena y trabaja con la información que necesitan los usuarios.

Pongamos un ejemplo, el sistema de información que gestiona el historial médico de los pacientes en un hospital. La información de este sistema procede de varias fuentes, principalmente de la que facilita el paciente y de los resultados de las distintas pruebas médicas a las que es sometido el paciente. Desde un punto de vista legal (esto depende de la legislación de cada país) la información del expediente médico es privada y solo el paciente y sus médicos, pueden tener acceso a ella. El problema de este planteamiento es que aunque la ley nos protege como pacientes, la realidad es que el acceso a nuestro expediente depende de lo sólida que sea la política de seguridad del sistema de información del hospital.

Si el hospital tiene un problema de seguridad en su sistema de información, nuestro expediente puede estar expuesto para que sea robado o lo que podría ser peor, para que sea modificado. La cuestión es que legalmente somos los propietarios de la información, pero desde el punto de vista de la tecnología no tenemos ningún control sobre la información de nuestro expediente médico, por la sencilla razón de que no tenemos acceso ni control de ningún tipo sobre la forma en la que el expediente está siendo gestionado.

Una solución podría ser que nosotros fuésemos los propietarios legales del expediente, pero que también controlásemos los permisos y accesos a esta información. Cambiaría la idea de cómo se gestiona la información, ya que ahora nosotros somos los auténticos propietarios de nuestra información y tendríamos la responsabilidad de gestionarla, ya

no delegaríamos la gestión de nuestros datos a un tercero, por ejemplo a un hospital.

Con blockchain podríamos almacenar nuestro expediente médico mediante transacciones encriptando los datos, para que solo nosotros podamos acceder a la información. Ahora imaginemos que vamos a un hospital y el médico nos solicita una prueba. Los resultados de la prueba no estarían almacenados en el sistema de información del hospital, la máquina que realiza la prueba, podría enviar directamente los resultados mediante una transacción encriptada a una red blockchain, el destinatario de esta transacción seríamos nosotros y solo nosotros podríamos acceder a los datos, porque estarían encriptados con nuestra clave pública.

Cuando fuésemos a la consulta del médico para ver los resultados, tendríamos la opción de visualizarlos en nuestra aplicación o bien, enviar los resultados mediante una transacción encriptada directamente al médico.

Es decir, somos nosotros, los pacientes, los que gestionamos la información de nuestro expediente médico y liberaríamos de esta forma al hospital de tener que gestionar la información de los pacientes. Este cambio en la percepción de quien es realmente el responsable de gestionar nuestra información es tremendamente profundo, ya que hasta ahora hemos delegado en un tercero, ya sea el banco, hospital, universidad, etc. Para que gestionase nuestra información. Una tecnología como blockchain cambia el papel que nosotros, los usuarios, tenemos dentro del actual esquema de gestión de la información. Ahora nosotros somos los auténticos propietarios de nuestra información.

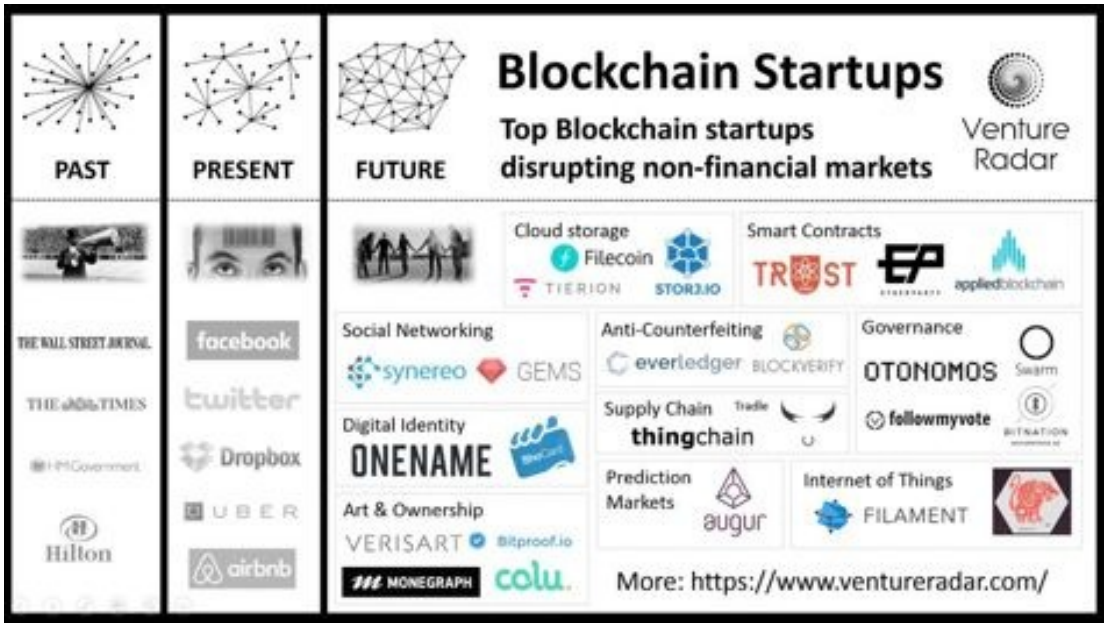
6
Hacia un futuro descentralizado

Un panorama descentralizado

Internet ha demostrado en los últimos 10 años que el modelo descentralizado será el que adopten las tecnologías de la información en el futuro. Hoy en día existe descentralización en la generación de la información, en la venta de productos/servicios, en la transmisión de la información, en la generación de las aplicaciones, etc. Es cierto que en algunos momentos todos esos mercados descentralizados confluyen en marketplaces comunes como puede ser el caso de YouTube para los videos, Amazon para la venta de productos, etc. Pero esos grandes marketplaces funcionan con información proveniente de puntos distantes del plante dándole forma al modelo descentralizado. De hecho, los números de Internet son tan grandes que resulta imposible concentrarlo todo y utilizar modelos centralizados.

Blockchain va a seguir contribuyendo a esa descentralización inevitable de las infraestructuras y la forma de proporcionar la información. La aportación más importante de blockchain es que va a conseguir descentralizar las entidades de confianza, algo impensable hace tan solo unos pocos años. Antes las entidades que controlaban la confianza, como los certificados electrónicos o las tarjetas de crédito, tenían un modelo centralizado, en el sentido en que toda la información era controlada sólo por unas pocas y no era accesible. Las tecnologías de blockchain permiten un cambio de paradigma importante en ese sentido ya que las entidades de confianza sencillamente no existen, en realidad se trata de una entidad de confianza distribuida y públicamente accesible.

Visto desde un punto global de pronto la confianza se va a convertir en global, las relaciones de confianza se van a poder establecer sin conocimiento mutuo y sin nadie que las regule, y además toda esa información va a tener un carácter público. Eso va a implicar unos profundos cambios en nuestra tecnología, pero también en nuestra sociedad y en la forma que se harán las coas. El modelo descentralizado mira al futuro, las entidades de confianza se van a ir desvaneciendo y esto afectará a la economía y los planteamientos sociales a nivel global.



Evolución de la descentralización en las aplicaciones (fuente: VentureRadar)

Seguramente esta situación quitará poder a los gobiernos y organizaciones, igual que la Internet de los años anteriores quitó poder a muchas grandes empresas. Pero es posible que existan algunas diferencias con el cambio de poder que se experimentó años atrás. Internet ha creado muchas grandes empresas que hoy en día están situadas en los primeros puestos del mundo. Tal vez esta nueva revolución no traiga grandes nuevas empresas, es posible que hasta cierto punto haga perder poder a alguna de las actuales. Esta vez la ganancia y la oportunidad es muy posible que se dispersen mucho más. Estamos entrando en un modelo de sociedad muy diferente al conocido hasta el momento. Lo cierto es que lo que ya se decía tiempo atrás sobre que Internet cambiaría gobiernos y sistemas sociales, es posible que ocurra con estas nuevas tecnologías. Como se decía en el capítulo 3, se trata de una revolución, no de una evolución.

La conexión con BigData

Big Data es una herramienta fundamental para el desarrollo de blockchain. De hecho blockchain no es otra cosa que una gran base de datos descentralizada, que permite consultar su contenido de manera pública, pero cuidado, eso no significa que los datos de los usuarios estén expuestos, significa que las transacciones son públicas, otra cosa es que el usuario quiera cifrar de alguna manera el contenido de una transacción, pero la transacción en sí es pública y esto es así porque de otra forma los nodos de una red blockchain no podrían validar las transacciones.

En este escenario en el que tenemos información pública de usuarios o máquinas realizando transacciones, Big Data puede ayudar a identificar patrones de comportamiento, por ejemplo para construir modelos predictivos. Estos modelos se pueden utilizar para un sin fin de propósitos, como por ejemplo identificar la aparición de brotes de alguna enfermedad analizando las transacciones que se realizan entre personas e instituciones médicas. O el interés real que despierta una nueva startup por la forma en la que se compran o vender participaciones.

Pero la aplicación más interesante de Big Data en blockchain es la construcción de modelos que permitan a los contratos inteligentes poder conocer patrones de comportamiento que les permitan tomar decisiones en función de lo que está ocurriendo. A día de hoy hablamos de contratos inteligentes, pero la realidad es que no deja de ser código que se ejecutan en función de unas entradas, por ejemplo, reciben una transacción y generan una salida, que pueden ser también transacciones. Es importante para el desarrollo de blockchain que este código que se ejecuta pueda conocer algo más del mundo que le rodea y nada mejor que utilizar Big Data para hacer a estos contratos algo más inteligentes.

Pero todo no son buenas noticias en cuanto a la aplicación de Big Data a blockchain, ya que existen algunas cuestiones que Big Data debe aprender a resolver, como por ejemplo la idea de que en un blockchain los usuarios no disponen de una identidad única, pueden generar cientos

o miles de pares de claves pública/privada de tal forma, que cada vez que generan una transacción lo hacen con una nueva clave pública/privada. Sería algo así como si en vez de utilizar la misma dirección de email para enviar todos nuestros correos, enviásemos cada email con una nueva dirección. Sería algo más complicado poder realizar un análisis de los datos si una variable como es el origen de la transacción tiene una enorme variabilidad.

Pero hay algo interesante en el tándem BigData-Blockchain, y es que como hemos visto en una sección anterior, con blockchain el modelo tradicional de la propiedad de los datos ha cambiado, desde el modelo de delegación de la gestión de la información, a un modelo en el que nosotros nos convertirnos en los auténticos propietarios de nuestra información. Lo interesante es que ahora somos nosotros los que podemos decidir qué información queremos ceder a un tercero para que la utilice, por ejemplo en campañas de marketing y lo que es más importante, tenemos la capacidad real para decidir si la información que cedemos/vendemos sea real o por el contrario esté anonimizada para mantener nuestra privacidad.

Internet de las Cosas

Según los principales analistas, la explosión de Internet de las cosas (IoT) en los próximos años tendrá un volumen tan grande, que sobrepasará la mayoría de las expectativas. De hecho Gartner cita los 25 mil millones de dispositivos conectados para el año 2020. ¿Pero cuál es el objetivo de que haya tantos dispositivos conectados? La respuesta es sencilla, necesitamos simplificar muchos de nuestros procesos diarios y para ello, necesitamos que las cosas que nos rodean, comiencen a ser cada vez más autónomas. Por ejemplo, si el coche que conducimos, ya incorpora un ordenador para controlar muchas de las funciones propias del coche, ¿por qué no se puede encargar el propio coche de solicitar la cita en el taller en el caso de que aparezca una alarma de posible avería? La realidad es que actualmente, la mayoría de nosotros, debemos interpretar un mensaje en el salpicadero de nuestro coche y solicitar nosotros mismos la cita con el taller.

Otro ejemplo típico para explicar la utilizar de IoT son los contadores del consumo eléctrico, hasta ahora el consumo se medía mediante contadores, los cuales había que leer y mandar esta información a la empresa que nos vende la electricidad, con lo que las lecturas suelen ser mensuales. Pero esto está cambiando gracias a los contadores inteligentes que se encargan de enviar nuestro consumo a la empresa eléctrica. Es decir, IoT debe dotar de más autonomía a las cosas que nos rodean, para simplificar nuestro día a día.

Pero IoT se enfrenta a varios problemas, los cuales debe poder resolver en los próximos años, porque de no ser así, el incremento de dispositivos conectados, puede convertirse en un problema realmente importante, queremos cosas más independientes e inteligentes, no queremos cosas que nos compliquen la vida.

Uno de los problemas a los que se enfrenta IoT es el de la seguridad de los dispositivos. Es importante que en todo momento, tengamos el control de las cosas que nos rodean, pensemos en un hogar conectado, en el que la mayoría de las cosas están conectadas, desde la tele a la lavadora. En este escenario, un problema de seguridad en los

dispositivos puede ser un problema realmente grave, ya que no solo alguien podría estar robando nuestra señal WIFI, sino que podría estar utilizando nuestras cámaras de seguridad o encendiendo la lavadora a su antojo.

El segundo problema al que debe hacer frente IoT es que la cosas conectadas, estarán intercambiando información con otras cosas y consumiendo servicios, por ejemplo, supongamos el caso de la lavadora inteligente que se encarga de avisar al servicio técnico para que venga a reemplazar una pieza, sería interesante que la propia lavadora pudiera realizar el pago de esa pieza, o por ejemplo la televisión pudiera comprar por nosotros los capítulos de nuestra serie favorita. Es decir, las cosas deberían poder realizar micropagos desatendidos para consumir servicios o bienes.

Y el tercer problema es que IoT no puede desarrollarse sobre un modelo centralizado de gestión de la información, en el que las cosas se comunican con nodos centrales para transmitir la información. Deben ser lo suficientemente independientes para poder comunicarse de manera autónoma y directa. No podemos depender de que un nodo central esté arriba para poder ver la tele o subir las persianas de nuestra casa. La descentralización de las comunicaciones en IoT es fundamental para no terminar muriendo de éxito.

La tecnología Blockchain puede ser una muy buena aliada para afrontar parte de los problemas de IoT. Volviendo a los tres problemas citados anteriormente, blockchain es tecnología segura, que garantiza la confidencialidad de los datos y los encriptamos, así como garantiza la autoría de todas las transacciones, es decir, nadie que no tenga nuestra clave privada, podrá suplantar nuestra identidad. Desde el punto de vista de IoT es importante que los dispositivos puedan confiar en la información que reciben del otro, por la sencilla razón de que solo el otro dispositivo puede firmar esa transacción.

El segundo problema, que los dispositivos puedan realizar micropagos, se puede solucionar gracias a blockchain, porque podríamos realizar transacciones directamente a un dispositivo y en ese momento, el dispositivo tendría saldo, para poder realizar sus propias transacciones.

Lo interesante de utilizar una tecnología como blockchain, es que el dispositivo no necesita tener acceso a nuestro banco para realizar pagos, somos nosotros, los que incrementamos el saldo del dispositivo en la red blockchain para que éste tenga saldo.

Y el tercer problema queda resuelto en cuanto que la tecnología blockchain se basa en un esquema descentralizado, en el que no existe un nodo central y por tanto, podríamos estar operando con los dispositivos de nuestras casas, aunque toda la red blockchain se hubiera caído.

La tecnología blockchain puede ser un gran aliado para que Internet de las Cosas se convierta en una realidad, simplificando gran parte de las soluciones y lo que es más importante garantizando la seguridad e integridad de la información con la que trabajan las cosas que nos rodearán.

Trazabilidad

En una economía global como la que tenemos, conocer el historial de un producto es una herramienta muy importante para la confianza del consumidor. Por ejemplo, actualmente podemos encontrar producto como la carne ecológica, en la que se asegura que dicha carne tiene unas propiedades determinadas y que procede de animales que han recibido un trato ecológico, desde la alimentación que se le ha facilitado, hasta las medicinas que ha recibido. El consumidor debe confiar en la propia cadena de suministros, ya que no tiene la certeza real de que esa carne sea realmente ecológica, es la propia confianza en la marca o el establecimiento donde la compra la que le asegura que está comprando un producto ecológico.

Como consumidores estamos acostumbrados a confiar en esta cadena de suministros, pero la realidad es que si alguien consigue saltarse la cadena de suministros, podemos recibir un producto de menor calidad, sin tener la menor conciencia de ello. Ahora supongamos que la trazabilidad de un producto no se basa en la confianza que tengamos en la propia cadena de suministro, sino en la información que recogemos de la etiqueta, supongamos que en el envase hay impreso un código QR que podemos leer fácilmente desde nuestro smartphone. Este QR es el código del producto y podemos utilizarlo para consultar en una red blockchain todas aquellas transacciones en las que aparezca nuestro código. Si todos los elementos que participan de la cadena de suministros, desde el ganadero que cría el animal, hasta la persona que recepciona el producto en el establecimiento, volcasen información referente a este producto en una red blockchain, sería muy fácil poder recomponer mediante transacciones, la información relativa a este producto en concreto y el consumidor podría comprobar no solo el historial del producto, sino la autenticidad de la información, ya que sería fácil descubrir fraudes al intentar manipular este tipo de información.

Mediante blockchain podríamos acceder de manera rápida y segura a toda la información relativa a un producto, como por ejemplo:

- La identidad del ganadero
- La fecha, lugar método de sacrificio del animal
- Datos del proceso de conservación.
- Controles sanitarios.
- Periodos del transporte.
- Controles de la cadena de frío.
- Fecha de recepción en el comercio.

Toda esta información podría estar accesible de manera transparente al consumidor, y la confianza de éste en el producto se basaría en la información que los distintos actores de la cadena de distribución han ido volcando en la red blockchain sobre el producto. Sería muy fácil para un consumidor, comprobar la autenticidad de un producto y la calidad del mismo.

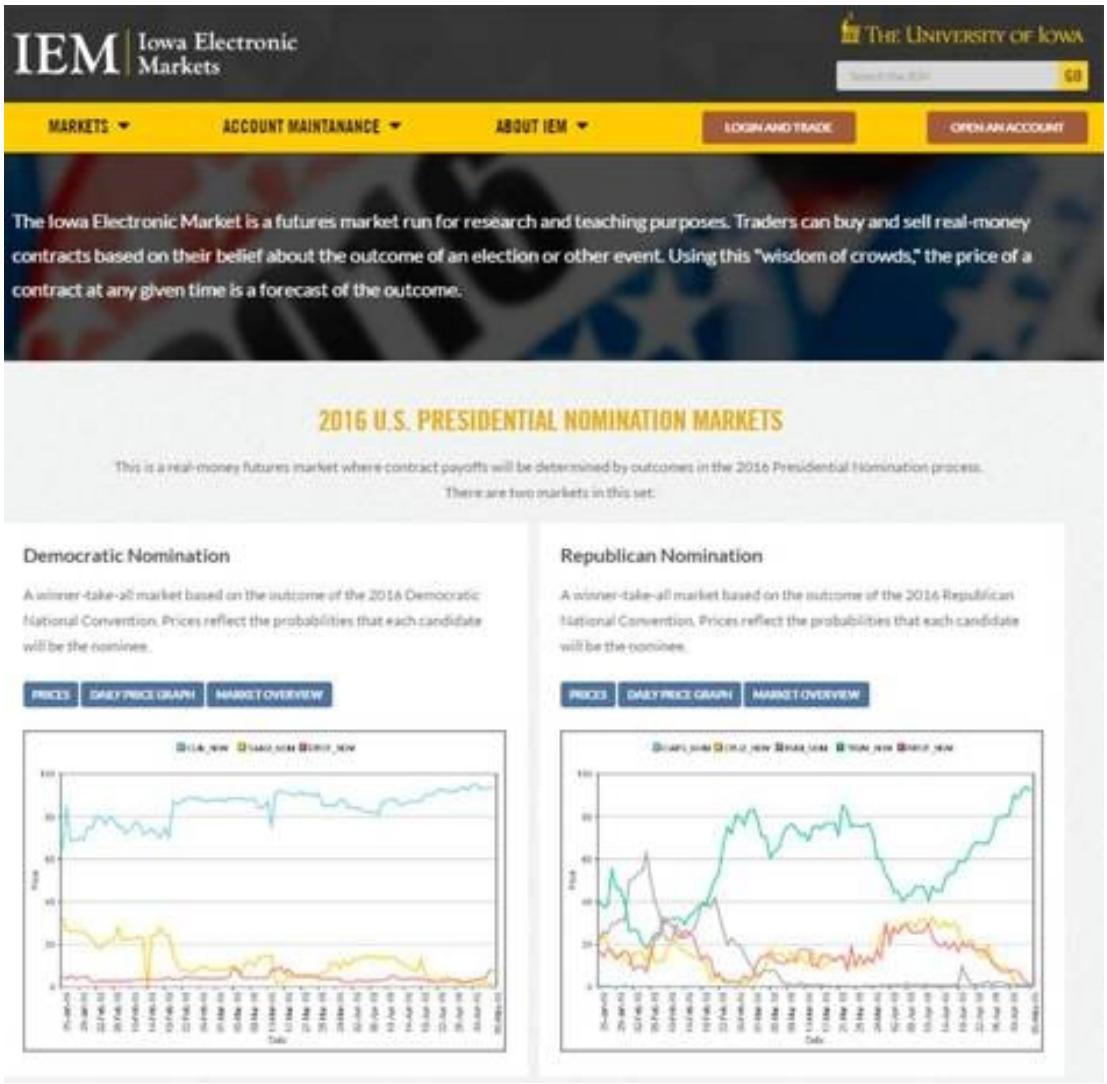
Mercados de predicción

Los mercados de predicción van a ser uno de los grandes protagonistas de los próximos años en su relación con la tecnología blockchain. Muchos de los smart contracts que se van a diseñar van a apoyar total o parcialmente sus decisiones en los datos que estos mercados, que mostrarán tendencias y situaciones futuras y que servirán para tomar decisiones de forma automática por parte de las DAS o las DAO/DAC a través de sus smart contracts. Tendrán más importancia que nunca antes. En gran medida el Big Data es una especie de mercado de predicción ya que es capaz de extraer datos ocultos y revelar verdades de la información que no se pueden deducir con facilidad. Pero Big Data por sí solo no reúne todos los requisitos de los mercados de predicción, partiendo de la base de que no está focalizado hacia la realización de predicciones, sino más bien hacia la extracción de datos que en muchos casos tienen más que ver con el pasado que con el futuro.

Los mercados de predicciones no son nuevos, existen desde hace varias décadas. Existe una gran evidencia empírica que demuestra que estos mercados realizan predicciones sobre sucesos futuros con un margen de error menor que los métodos convencionales. En gran medida esto se corrobora por el hecho de que juntar opiniones sobre sucesos futuros utilizando dinero en muchos casos para enfrentar dichas predicciones, hace que los participantes estén generalmente muy bien informados y por tanto puedan aportar unos grados de fidelidad a lo que puede ocurrir bastante altos.

Por ejemplo el mercado de electrónica de la Universidad de Iowa (http://tippie.uiowa.edu/iem/) es uno de los más populares del mundo. En dicho mercado se pueden encontrar predicciones que van desde las elecciones presidenciales americanas hasta la política de la reserva monetaria. Es un mercado que funciona de forma automática y se actualiza cada 15 minutos. Otro mercado de predicciones es el Hollywood Stock Exchange (http://www.hsx.com/) donde se realizan predicciones relacionadas con el mundo cinematográfico. Google tiene

su propio mercado de predicciones interno utilizando Gobbles (moneda virtual) donde los empleados apuestan por las ventas de un producto particular o de cómo le irá a la empresa durante un determinado tiempo futuro. Esta información es muy valiosa para Google tanto a nivel de poder medir el optimismo de sus empleados como para contemplar escenarios que no hayan sido previstos por ejemplo a la hora de poner a la venta un producto. Microsoft es otra empresa con un mercado de predicciones interno (InformationForecasting Exchange), que ha utilizado desde el año 2006 para comprobar si se están alcanzando las planificaciones y objetivos por una parte y para predecir fallos o problemas en productos futuros por otra. Los sitios webs de apuestas convencionales que han surgido en Internet en los últimos años son mercados de predicciones igualmente.



Predicción de la elección de candidatos para las elecciones americanas 2016 en el mercado de electrónica de la Universidad de Iowa

Augur (http://www.augur.net/) es un mercado de predicciones en Internet muy heterogéneo en el sentido de que reúnes predicciones muy diversas que funciona sobre el blockchain de ethereum y utiliza su propia moneda virtual REP (por reputations). En agosto de 2015 Augur realizó una subasta pública de acciones (crowdsale) que le permitió levantar una financiación para el proyecto de 5,3 millones de dólares. El mercado de predicciones de Augur funciona de la misma manera que los convencionales en Internet, con la diferencia de que aquí las predicciones son propuestas directamente por usuarios que esperan la entrada de otros usuarios que acepten los retos de las predicciones.

Es muy probable que en el futuro se utilicen estos mercados de predicciones como uno de los apoyos en la toma de decisiones por parte de los smart contracts. Si en el mundo real, el director de una empresa tiene que tomar decisiones casi diarias y en muchos de los casos con muy poca información y rodeado de circunstancias personales que pueden hacer perder perfección al proceso deductivo, la posibilidad de aplicaciones capaces de tomar decisiones alimentándose de datos del mundo real y realizando análisis por medio de algoritmos previamente consensuados, no parece una barbaridad, de hecho puede llevar a decisiones más sensatas que en el caso anterior. Es cierto que estas decisiones serán automáticas, producto de algoritmos, pero tendrán en cuenta datos pasados unidos a predicciones futuras con una velocidad y riqueza de fuentes de información difícilmente igualables. Otro factor a tener en cuenta será la velocidad. El ser humano es capaz de tomar decisiones que en muchos casos puede superar a las de las máquinas por circunstancias relativas fundamentalmente al estado emocional y a las sensaciones con respecto a una determinada operación. Esto no es posible en el caso de algoritmos, pero por el contrario el algoritmo ejecuta a una velocidad imposible para el ser humano aparte de la temporalidad de estas decisiones. Un algoritmo no duerme, por tanto puede tomar decisiones 24 horas al día. En el caso de cualquier empresa, por muy rápido que puedan reacciones, una simple cuestión burocrática y geográfica aleja cualquier opción de toma de decisiones con esta capacidad temporal

con esta capacidad temporal.

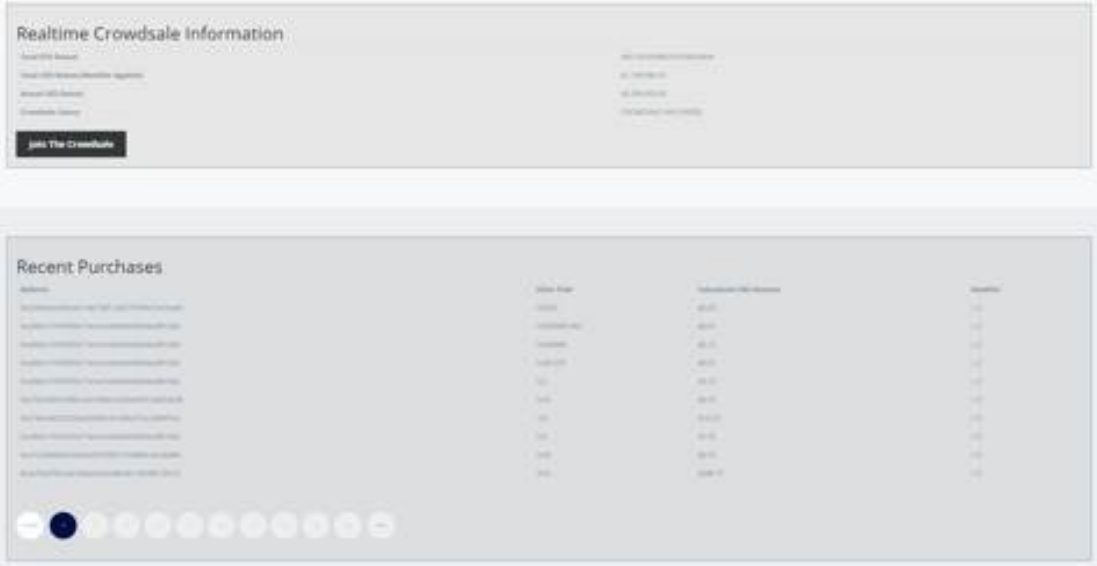
Crowdsales

Aunque ya se ha hablado con anterioridad de las crowdsales en el libro, su importancia y la que seguramente tomarán en el futuro merecen una consideración especial.

Las crowdsales son los mecanismos de financiación que emplean en la actualidad las DAO/DACs para la puesta en marcha de sus estructuras en forma de una o varias dApps. Una crowdsale es como una venta pública de acciones de la empresa en forma de tokens de su blockchain. Es decir, cuando una DAO quiere obtener financiación para la realización de su proyecto destinará un porcentaje de sus tokens a una crowdsale. Si el dinero recaudado en esa crowdsale se ajusta a los mínimos establecidos, el total de tokens que se han puesto a la venta se dividirán entre el número de personas que aportaron dinero a esa crowdsale obteniendo cada participante un número de tokens proporcional al dinero aportado. Normalmente los organizadores de la crowdsale habrán apartado previamente un porcentaje de tokens destinados a ellos mismos y a los desarrolladores. A partir de ese momento la DAO/DAC tiene vida propia, está gobernada por una serie de accionistas que ostentan una parte de sus acciones y funciona mediante smart contracts que pueden ser modificados por acuerdo entre todas las partes. En función de lo bien o mal que vaya la iniciativa el valor del token irá subiendo o bajando y por tanto la rentabilidad de la inversión realizada. Estos tokens pueden ser comprados o vendidos por sus poseedores con simples transferencias realizadas a través de la blockchain correspondiente al proyecto.

Ethereum es en la actualidad el blockchain mejor preparado probablemente para la realización de crowdsale. La documentación disponible a través de la propia web (https://www.ethereum.org/crowdsale/) proporciona con bastante detalle el mecanismo de realización de una crowdsale. Sin embargo, existen ya herramientas que pueden facilitar bastante la realización de la misma. Tal vez la más popular sea Coinsprim (https://www.coinprism.com/) o Crowdsale.co (http://crowdsale.co/), una empresa de Denver que

desarrolla toda la consultoría y ejecución de una crowdsale.



Finalización de la crowdsale de Digix en abril de 2016 con un total de 5.500.000$ obtenidos en 4 horas

Una polémica en torno a las crowdsales es la protección del inversor. El sentido de una crowdsale es muy diferente a las de las operaciones tradicionales de crowdfunding, ya que en este caso el inversor compra participaciones en la empresa. Mientras que habitualmente la compra de participaciones en una empresa está fuertemente regulada en cualquier país, como es el ejemplo de la CNMV para el caso del mercado español o la SEC para el caso del mercado americano, la regulación para una crowdsale es nula y en consecuencia la protección del inversor es inexistente. Ya se han dado casos como el ejemplo de BitFunder, cerrado por presiones de la SEC americana sobre las operaciones que estaba llevando a cabo en relación a las crowdsales.

La web 3.0

Blockchain se ha identificado a menudo con la nueva “versión” de la web tras la web 2.0 que tomó forma en el año 2005 a partir de los postulados de Dale Dougherty (http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html).

Tras el despegue del concepto web 2.0 y todas sus tecnologías asociadas, ha habido numerosos desarrollos, experiencias de usuarios e iniciativas que se han autoproclamado como la nueva web o la web 3.0. No es más que un nombre, pero la reflexión sobre las características de blockchain y el hueco que cubre a nivel de infraestructuras de confianza puede llevar a pensar que realmente se trata de una revolución en la web.

La web 2.0 trajo la democratización de la información a través del fenómeno de los prosumidores. De repente cualquier usuario se podía convertir en generador de información, una circunstancia exclusiva de grandes empresas hasta ese momento. La irrupción de los blogs, los entornos de gestión de contenidos en la web o los sitios de subida de contenidos como Youtube o las redes sociales permitieron una web muy diferente a la que se había conocido hasta el momento. Esta democratización fue sólo de información, el resto de aspectos quedaron intactos como ya se comentaba al principio de este libro. Blockchain democratiza los pagos y el sentido de la confianza entre pares de una manera descentralizada. Es hasta cierto punto similar a lo que hizo la web 2.0 con la información, pero en este caso se trata de pagos y de gestión de activos. La web 2.0 consiguió en su día que la producción y la gestión de la información a nivel de la web superara a la del mundo convencional y que muchos servicios del mundo real como la producción de música o libros quedaran emulados en este nueva forma de web con nuevos modelos de negocio desconocidos hasta ese momento y mucho más democráticos y globales.

La nueva web que proclama blockchain integra las tecnologías de confianza a través de un modelo de gestión propio, exclusivo de la red y

desconocido hasta el momento. En la actualidad ya podemos ver proyecto que van integrando las funciones de blockchain con las de la web tradicional. Por ejemplo Blockai (https://blockai.com/), un proyecto que proporciona extensiones y capacidad web para reclamar la autoría y/o propiedad de obras conforme se navega por Internet. La integración de las carteras en los navegadores tradicionales es ya posible con extensiones como MyWallet (https://blockchain.info/es/wallet/browser-extension) desarrollada por Blockchain.info y disponible para navegadores como Google Chrome. Esta extensión incorpora una cartera de bitcoins a la navegación y permite el pago en los sitios autorizados. La aplicación Persona, de Consensys (https://consensys.net/) es otro ejemplo de integración de identidad y de información relativa a los pagos dentro de los navegadores. Su sistema de identidad personal uPort permitirá la gestión de identidades y la creación de carteras web para cualquier navegador.

Las aplicaciones mencionadas anteriormente son sólo una pequeña representación de todo el ecosistema que se está desarrollando en torno a la web 3.0. Este nuevo paradigma de relación en la web no pretende eliminar completamente las entidades de confianza del mundo tradicional que utilizamos actualmente, simplemente va a racionalizar el uso de forma que cada uno va a tener su papel. Igual que el correo electrónico no eliminó el correo tradicional, las tecnologías blockchain no van a eliminar las entidades de confianza tradicionales. Simplemente habrá casos donde no tenga sentido el uso de entidades de confianza del mundo real y otras donde sí, igual que hay determinados tipos de información que se envían utilizando correo electrónico y no tiene sentido enviarla de otra manera y hay otras ocasiones donde el correo convencional es lo más apropiado. La compra/venta de activos digitales y la autoría de los mismos será regulado en el futuro por las tecnologías blockchain, pero seguirá habiendo entidades de confianza del mundo real como los informes meteorológicos, los datos poblaciones de los países, la gestión del dinero fiat, etc, que utilizarán entidades de confianza del mundo real. La web 3.0 cambiará la sociedad y la economía igual que la web 2.0 cambió el mundo de la generación y distribución de la información, pero lo va a hacer en los sitios donde este cambio tiene sentido y es razonable a todos los niveles. Corresponderá a la comunidad ir poniendo a cada uno en su lugar, utilizar unos medios

la comunidad ir poniendo a cada uno en su lugar, utilizar unos medios para unos propósitos y otros medios para otros.

Aparte de todo lo comentado anteriormente, como ya ocurrió con la web 2.0, se irán vislumbrando nuevos modelos de negocio imposibles hasta el momento. Se han comentado ya algunos de ellos en capítulos anteriores en forma de aplicaciones distribuidas, DAO/DAC y las DAS. En muchos casos se trata de transformaciones de negocio desde el mundo convencional al mundo de Internet como es el caso de la popular Bitcoin, en otros casos sin embargo se trata de modelos de negocio imposibles hasta el momento como son los casos de todo el conjunto de aplicaciones distribuidas que propone Ethereum.

Conclusiones

A lo largo de este libro hemos tratado de reflejar la realidad y el futuro de blockchain. El protagonismo adquirido en los últimos años por Bitcoin está siendo sustituido por su protocolo blockchain. En numerosos medios de comunicación hemos podido ver durante los últimos meses discursos y afirmaciones sobre las ilimitadas posibilidades de blockchain, no solamente en el sector financiero, sino en cualquier otro entorno donde haya que custodiar y/o traspasar activos. Numerosos bancos como DBS, Santander, ING, BBVA, Bankinter, Goldman Sachs, por nombrar solamente unos pocos, han anunciado ya que están experimentando con esta tecnología.

No obstante las evidencias son todavía pocas. Tengamos en cuenta que la capitalización de la moneda digital no llega a los 9 mil millones de dólares, una propina si hablamos del entorno económico global. Las aplicaciones no han hecho más que empezar a experimentar, tanto a nivel fintech como a otros niveles relativos al blockchain 2.0. Si observamos el prestigioso Hype Cycle de Gartner sobre tecnologías emergentes, en el año 2014 las criptomonedas estaban situadas en el pico de las expectaciones infladas, es decir, mucha gente hablaba de ellas, pero nadie sabía exactamente qué hacer con las mismas. En el mismo gráfico de julio de 2015 las criptomonedas están cayendo hacia el valle de la desilusión (curva baja de la gráfica), donde ya se encuentran los exchange de criptomonedas (casas de cambio entre divisas virtuales), con unas expectativas de entrada en mercado de entre 2 a 5 años, mientras que las propias criptomonedas tienen unas expectativas de llegada al mercado de consumo de entre 5 a 10 años. Seguramente estas cifras se acortarán algo, pero muestran un panorama todavía de algunos años hasta su consolidación en nuestras vidas.

Hasta entonces queda un período de experimentación por parte de la industria, de intentos fallidos, de crowdsales fracasadas y de criptomonedas que no prosperarán. Pero a pocos cabe ya duda de que blockchain ha llegado para quedarse, que no se trata de una tecnología que se haya puesto de moda, que no es una especulación fantasiosa hacia un futuro tecnológico poco imaginable y que aborda una necesidad

que nadie había sido capaz de solucionar hasta el momento.

Por todo ello, pensamos que hay pocas dudas sobre su consolidación, aunque tampoco pensamos que blockchain y su ecosistema de criptomonedas vayan a causar la desaparición de la moneda real, ni siquiera en el largo plazo, como el correo electrónico no ha hecho desaparecer al correo tradicional o los diarios electrónicos no han hecho desaparecer a los de formato convencional. Blockchain seguramente ocupará el hueco que le corresponde en la gestión de activos digitales, entendiendo por tales tanto las transferencias monetarias como la de otros bienes, pero seguramente no tendrá cabida en el mundo real donde la moneda fiat, con un formato tal vez más digital y moderno, como la ausencia de papel, seguirá dominando las estructuras económicas.

No obstante lo anterior, la revolución de blockchain es diferente a la que protagonizó la web 2.0, porque va a golpear los modelos económicos que forman parte de las estructuras más básicas de nuestra sociedad. ¿Cómo dominarán los gobiernos estas tecnologías? ¿Cómo se adaptará la industria financiera a esta nueva forma de hacer las cosas? ¿Supondrá el nacimiento de nuevos gigantes que no existen en la actualidad como ocurrió con Google, Facebook, YouTube o Yahoo!? Son preguntas difíciles de contestar. Nos encontramos ante una tecnología todavía inmadura y difícil de implantar. Las grandes instituciones tienen en la actualidad un profundo respeto por cualquier tendencia digital y son conscientes de la importancia de blockchain. De hecho los bancos son las entidades que más están apostando por esta tecnología, aunque sea de momento a nivel más experimental que real. Es probable que los gobiernos mundiales se vean amenazados si la tecnología va prosperando como está proyectado, y seguramente tratarán de dificultar inicialmente, legislar posteriormente y convivir finalmente. Su participación será más intervencionista cuanto mayor sea la amenaza que vayan percibiendo.

Por nuestra parte nos queda la impresión de que prácticamente todo está aún por hacer. Pensamos que el mundo que nos enseñará blockchain en los próximos años serán tan inimaginable y lleno de

sorpresas como fue el que dibujaron los protocolos del origen de Internet en su día. Será un mundo lleno de oportunidades, que traerán nuevas amenazas.

Pero entendemos que no va a ser una opción, como no lo han sido las tecnologías digitales que han aparecido en los últimos años y que han cambiado nuestra sociedad.

APÉNDICE: DIRECCIONES WEB

Se adjunta a continuación la relación de direcciones web que han sido utilizadas en la redacción de este libro con una pequeña descripción de las mismas:

Augur - Apuestas y mercado de predicciones utilizando moneda propia (http://www.augur.net/)

Bit2me - Compra y venta de bitcoins (http://www.bit2me.com),

BitHalo - Smart contracts (https://bithalo.org/),

Bithandle - Registro con direcciones Bitcoin (http://www.hackathon.io/bithandle)

BitID - Identificación con direcciones Bitcoin (http://bitid.bitcoin.blue)

Bitshares - Acceso universal a contratos inteligentes para la inclusión de nuevas características (http://www.bitshares.org)

Blockai - Gestión de copyright (https://blockai.com/)

Código Namecoin - https://github.com/namecoin

Codius - Herramientas de desarrollo smart contracts (https://codius.org/),

Coinbase - Envío de bitcoins y gestión de wallets (http://www.coinbase.com)

Coinsprim - Monedas coloreadas (https://www.coinprism.com/)

Cómo conseguir Namecoins - https://wiki.namecoin.info/index.php?title=How_to_get_Namecoins

Consensys - Desarrollo de aplicaciones distribuidas (https://consensys.net/)

Counterparty - Herramientas financieras en redes Bitcoin (http://counterparty.io/)

Crowdsale – Ventas masivas en Ethereum (https://www.ethereum.org/crowdsale/)

Crowdsale.co - Gestión y organización de crowdsales (http://crowdsale.co/)

Dale Dougherty – Principios de la web2.0 (http://www.oreilly.com/pub/a/web2/archive/what-is-web- 20.html)

Dash - Transacciones instantáneas con criptomonedas (http://www.dash.org)

D-cent - Herramienta para democracia directa por parte de los ciudadanos (http://tools.dcentproject.eu/)

Digix - Plataforma financiera para el estándar del Oro (http://www.digix.io)

Dominio bit - Registro de direcciones (http://www.dobit.me)

eMunie - Creación y desarrollo de criptomonedas (http://www.emunie.com)

Eris Industries - Desarrollo de aplicaciones blockchain (http://erisindustries.com)

Factom - Protocolo bitcoin 2.0 (http://www.factom.org/)

Filament (Pinoccio) - Sensores para recolección de datos a nivel industrial (http://filament.com)

Getgems - Dapp al estilo Whatsapp y Telegram (http://etgems.org)

Hawk - Almacenamiento cifrado de transferencias económicas (http://oblivm.com/hawk)

Hollywood Stock Exchange - Mercado de predicción (http://www.hsx.com/)

IDNI - Inteligencia artificial basada en razonamiento y ontologías (http://www.idni.org)

IOTA - Internet de las cosas – (http://www.iotatoken.com)

La'Zooz - Sistema descentralizado de transporte, similar a Uber. (http://www.lazooz.org)

Localbitcoins - Compra y venta de bitcoins (http://www.localbitcoins.com)

Mercado de capitalización de monedas digitales - http://coinmarketcap.com/

Mercado de electrónica de la Universidad de Iowa - (http://tippie.uiowa.edu/iem/)

Monegraph – Gestión y descripción de la moneda (http://www.monegraph.com)

Monegraph – Plugin para wordpress (https://es.wordpress.org/plugins/monegraph)

Monegraph Inspector - (https://monegraph.com/inspect)

MyWallet – Wallet para bitcoin (https://blockchain.info/es/wallet/browser-extension)

Namecoin – Registro digital de nombres de dominio .bit

(https://namecoin.info/)

Nxt - Desarrollo de aplicaciones descentralizada (http://www.nxt.org/)

OneName – Base de datos global para personas y empresas (http://www.onename.com)

OpenBazaar - Comercio B2C (http://www.openbazaar.org)

Orisi - Pago por servicios de hosting sobre Oracle (http://orisi.org)

Peercoin – Moneda digital segura y sostenible (https://peercoin.net)

Ripio – Wallet con medidas adicionales de seguridad (http://www.ripio.com),

Ripple - Desarrollo de herramientas para instituciones financieras y sistemas de pago (http://www.ripple.com)

RootStock – Plataforma de smart contracts bajo bitcoin (http://www.rootstock.io/).

Sidechain (blockstream) - Interoperabilidad entre diferentes blockchains (http://blockstream.com/)

Slock.it - Gestión de apertura de puertas utilizando blockchain (http://www.slock.it)

SolarCoin - Valoración de la generación de electricidad vía energía solar (http://www.solarcoin.org/)

Storj - Almacenamiento descentralizado. Similar a Dropbox. (http://storj.io)

Stripe – Gestión online de pagos (https://stripe.com)

Supernet - Plataforma de criptoservicios (http://www.supernet.org)

Synereo- Red social de características similares a Facebook (http://www.synereo.com)

Twister - Un Twitter descentralizado (http://twister.net.co)

Validating Satoshi (OrNot) - Artículo por Dan Kaminsky (https://dankaminsky.com/2016/05/02/validating-satoshi- or-not/)

Waves - Creación de tokens y comercio descentralizado (http://ico.wavesplatform.com)