La seguridad de blockchain como disrupción global para bitcoin y otras aplicaciones

» Alejandro Mario Hernandez
CAETI – Universidad Abierta Interamericana, Universidad Nacional de Rosario, Argentina
AlejandroMario.Hernandez@UAI.edu.ar

Fecha de recepción: 1 de febrero de 2019.
Fecha de aceptación: 1 de junio de 2019.

Resumen

En este artículo, hacemos un pantallazo general a una tecnología innovadora que está dando mucho que hablar alrededor del mundo. Esta tecnología, denominada blockchain, le da sustento a la moneda virtual por excelencia, el bitcoin, y es un poco gracias a esto que ha ganado mucho reconocimiento a nivel global. Sin embargo, el bitcoin no es más que una de un sinnúmero de aplicaciones que pueden cambiar radicalmente gracias a blockchain. Este cambio es básicamente un nivel de seguridad sustancialmente superior a todo lo previamente conocido. Con esto, blockchain se transforma en una las tecnologías más disruptivas de los últimos tiempos. En el artículo también mencionamos algunos de los puntos que deben seguir siendo mejorados con respecto a la tecnología, para lograr transformarla en algo que perdure en el futuro.

PALABRAS CLAVE: CADENA DE BLOQUES, SEGURIDAD, CONTRATOS INTELIGENTES, APLICACIONES.

Blockchain security as a global disruption for bitcoin and other applications

Abstract

In this article, we skim through an innovative technology that is being talked about throughout the World. This technology, known as blockchain, gives infrastructure to the most known virtual coin, the bitcoin, and it is thanks to this that the technology has gained lot of attention globally. However, the bitcoin is just one of an uncountable set of applications that can radically change thanks to blockchain. This change is basically a level of security substantially higher than everything previously known. With this, blockchain becomes one of the most disruptive technologies of the last years. In this article we also mention some of the points that must continue to evolve with respect to the technology, for transforming blockchain in something that lasts in the future.

KEYWORDS: BLOCKCHAIN, SECURITY, SMART CONTRACTS, APPLICATIONS.

1. Introducción

Desde hace algunos años, el bitcoin está ganando titulares en los diarios de todo el mundo (Nakamoto, 2008).[1] Muchos pueden pensar que es una moneda, algunos que es simplemente una burbuja, incluso hay gente que piensa que es una tecnología. Sin embargo, el bitcoin no es más que una aplicación (de una tecnología disruptiva conocida como *blockchain*) (infotechnology.com, 12/8/2016).

Esta aplicación, debido a su forma de funcionamiento, hace que mucha gente se interese en colaborar en dicho funcionamiento, y como recompensa esta gente recibe acceso a poder controlar partes de bitcoins que son "emitidos". Esta última palabra está entre comillas, ya que el bitcoin no proviene de ningún banco central, con lo cual no es realmente emitido, si no que simplemente el acceso al mismo es a través de una clave, que permite al que la conoce poder "transferirlo" a otra persona. Así, disponer de claves de bitcoin hace que uno tenga algo que puede tener un cierto valor, que a la vez puede ser usado para intercambiar con algún producto o servicio, y esto hace que se confunda con una moneda.[2] Sin embargo, el real "resguardo de valor" de bitcoin no es más que la expectativa de toda la gente que lo utiliza en que cada vez más gente lo vaya a utilizar, y que lo vaya a aceptar para intercambiar por cada vez más productos y servicios.

Mas allá de esto, los usuarios de bitcoin tienen plena confianza en la tecnología que lo sustenta, el blockchain, que lo hace prácticamente inviolable. En efecto, el blockchain es una tecnología que es realmente disruptiva, y bitcoin no es más que la primera aplicación que corre sobre la misma. De hecho, blockchain nació con la aplicación bitcoin, pero como veremos en el presente artículo, la tecnología puede ser utilizada, y ya lo está siendo, para muchísimas otras aplicaciones. Haciendo un parangón, la aplicación WhatsApp corre sobre Internet, pero existen muchísimas otras aplicaciones, y podrían existir muchas que ni nos imaginamos, más allá de que WhatsApp sea posiblemente una de las más famosas y más utilizadas en la actualidad (unocero.com, 25/1/2019).

Con esto, podemos comenzar a mencionar qué es la tecnología blockchain, y para esto damos una serie de características definidas por la misma:

1. Lo primero que define blockchain es una estructura de datos. Con esto, todos los datos almacenados en una blockchain deben seguir una determinada configuración.
2. También se define un algoritmo para el almacenamiento de los datos. Así, cada vez que se deban almacenar datos nuevos, y más allá de que los mismos deban seguir una determinada configuración, los mismos deben ser almacenados siguiendo una serie de etapas para lograr dicha configuración.
3. Se define un protocolo de comunicación entre los participantes, de forma tal que todos los dispositivos conectados a la blockchain puedan compartir datos y "entenderse".
4. Por último, se define un **protocolo de consenso** para poder determinar datos válidos y datos inválidos, y así poder resguardar los datos de blockchain de cualquier posible ataque. Como dijimos, la seguridad provista por blockchain es sustancialmente superior a todo lo previamente conocido, y más adelante veremos que el protocolo de consenso es lo principal para lograr esto. A su vez, el protocolo de consenso forma parte de la gran idea que tuvieron los creadores de bitcoin, y de esta tecnología

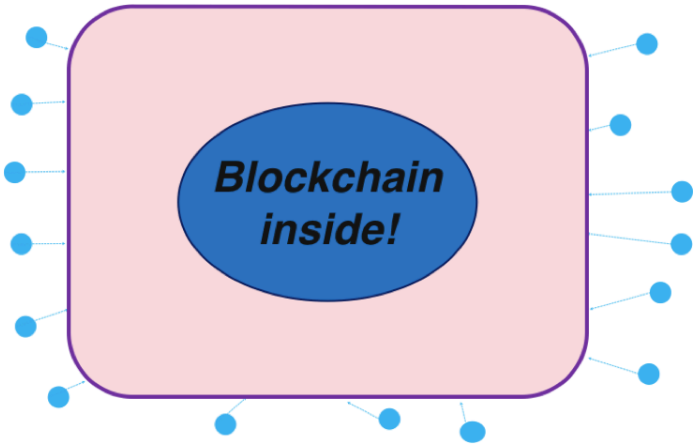
1 https://www.nytimes.com/topic/subject/bitcoin. Accedido el 25/05/2019.
2 https://es.wikipedia.org/wiki/Moneda_(divisa). Accedido el 25/05/2019.

que lo sustenta. Estos creadores están agrupados bajo el pseudónimo de Satoshi Nakamoto, y más allá de que su idea original fue crear una aplicación, el bitcoin, quizá no imaginaron que la infraestructura que crearon luego podría ser utilizada para un sinnúmero de otras aplicaciones.

En el resto del presente artículo, nos enfocaremos primero en terminar de entender qué es blockchain y también cómo se usa. Luego, metiéndonos en algo un poco más técnico, pero tratando de no dejar de ser legible aún para el lector menos especializado, vamos a ver qué son las transacciones de blockchain, cómo son almacenadas en una red *peer-to-peer*,[3] y los detalles de los protocolos de comunicación y de consenso. Por último, hablaremos sobre el ecosistema actual de blockchain, que fundamentalmente está basado en un nuevo concepto conocido como *contratos inteligentes*,[4] y las aplicaciones que gracias a esto pueden ser desarrolladas: mencionaremos tanto aplicaciones existentes, como así también aplicaciones que se encuentran en desarrollo y posibles futuras aplicaciones.

2. Qué es y cómo se usa blockchain

Blockchain es una computadora (Yahya, Chen, 2019). Es una computadora a la que todo el mundo puede conectarse, utilizarla, y guardar información en la misma. Pero no es una computadora similar a la que estamos acostumbrados. No es una laptop, ni una desktop, ni un smartphone ni tablet, ni siquiera es un servidor o un cluster de CPUs. El siguiente es un diagrama que esquematiza este concepto:



Ahora bien, cuando se requiere que un sistema cumpla con las siguientes condiciones, es cuando conviene utilizar esta computadora:

» Que existan muchos participantes compartiendo los datos. La blockchain nos permite que todos vean lo mismo.
» Que muchos participantes tengan que estar habilitados para cambiar los datos. La blockchain nos permite que se guarden correctamente.

3 https://es.wikipedia.org/wiki/Peer-to-peer. Accedido el 25/05/2019.
4 https://es.wikipedia.org/wiki/Contrato_inteligente. Accedido el 25/05/2019.

» Que se requiera verificabilidad de los datos y de los procesos por los cuales fueron guardados. La blockchain le da confianza sobre esto a los participantes, aún cuando no confíen entre ellos.
» Que se requiera eliminar intermediarios. La blockchain permite llevar adelante esto, logrando reducir costos, tiempo de conciliaciones, etc.
» Que se necesite eliminar interacciones. La blockchain nos permite esto, ahorrando tiempo.
» Que las transacciones deban tener interrelación entre ellas, ya sea dependencia mutua o dependencia múltiple. La blockchain mantiene toda esta información.

A su vez, esta computadora no se utiliza por sí sola, sino que se integra con el resto de las computadoras. De esta manera, una aplicación distribuida (medium.com, 16/10/2019) basada en blockchain tendrá una arquitectura (Bass, Clements, Kazman, 2012) en la que se utilice la computadora blockchain para manejar la información que requiera cierto grado de seguridad, quizá un servidor para la manipulación de los grandes datos, una laptop para administrar el servidor, y por último un smartphone para interactuar con la aplicación.

3. Cómo funciona blockchain

3.1. Transacciones

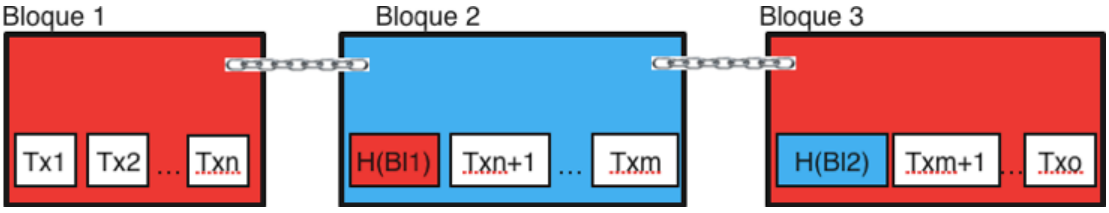
Dijimos que blockchain es una computadora, y ahora podemos decir que blockchain es una computadora en la cual se guarda información sobre *transacciones*. Ahora bien, una transacción es en definitiva cualquier dato que merezca ser guardado, ya sea para reflejar un evento, un suceso o algún cambio que represente algo en el sistema que está siendo utilizado. Los siguientes son algunos ejemplos de transacciones en distintos tipos de sistemas:

» La información de que X le pasó dinero a Y. En efecto, cuando alguien le pasa dinero a otro, es necesario saber a quién pertenece el dinero a partir de ese momento.
» El nombre del nuevo dueño de una casa. En efecto, si un sistema informático guarda información relevante en cuanto a propiedades de bienes raíces, es necesario que esté reflejado con precisión. Si pensamos en un sistema no informatizado, podríamos decir que las escrituras son justamente las transacciones que reflejan este suceso.
» La ejecución de un programa. En efecto, si tenemos que registrar los programas que fueron y son ejecutados, la ejecución de uno en particular es la transacción básica a guardar.
» Una foto de una luna de Júpiter. Si tuviéramos un sistema que mantiene históricamente la evolución de los astros, una foto puede capturar el momento en el cual se produce el evento de interés.
» El nombre del autor de una canción o libro. Si queremos mantener información de *copyright*, el nombre del autor es el suceso que nos permite asegurar esto.

Ahora bien, cuando tenemos un conjunto de transacciones que reflejan eventos temporalmente cercanos, las agrupamos todas juntas en un bloque. Las transacciones no necesariamente son interdependientes, pero se guardan juntas por ser (casi) simultáneas. Luego de esto, calculamos una huella (obtenida utilizando el mecanismo matemático de *hash criptográfico*),[5] y la agregamos como la transacción inicial del siguiente conjunto de transacciones. La huella de un bloque es en este caso un evento que merece ser guardado, similar a los ejemplos anteriores. Por ende, esta huella va a terminar siendo guardada en el siguiente bloque. De esta manera,

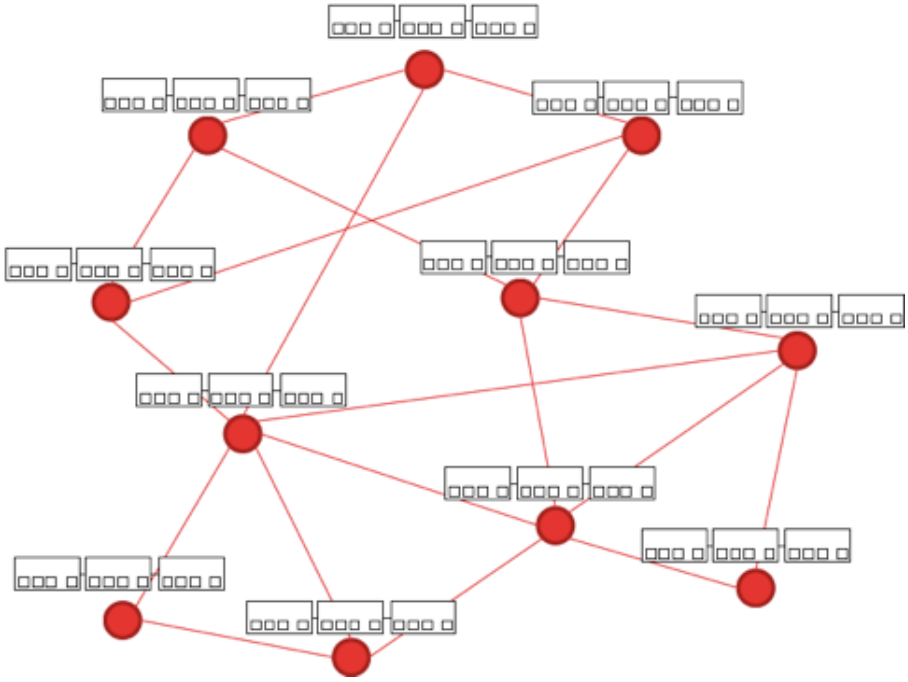
5 https://es.wikipedia.org/wiki/Funci%C3%B3n_hash_criptogr%C3%A1fica. Accedido el 25/05/2019.

tenemos un encadenamiento de bloques (de acá el nombre *blockchain*, que en inglés significa *cadena de bloques*), que puede ser esquematizado con el siguiente diagrama:



3.2. Red p2p

La cadena de bloques que mencionamos, se encuentra replicada en muchas computadoras físicas alrededor del mundo, denominadas *nodos*, como esquematiza el siguiente diagrama:



Así es como se compone la computadora *lógica* blockchain. Y esta computadora, compuesta de tantas piezas de hardware reales, hace que la seguridad sea sustancialmente superior a todo lo conocido. En efecto, ante cualquier problema que tenga alguno de los nodos (ya sea por algo involuntario, por un error, por un ataque, o por lo que fuere), existen muchas otras copias de los datos en el resto de los nodos. El estado global de la blockchain, es el que consta en la mayoría de los nodos (esto es, el 50% más un nodo). Así, están cubiertos tanto la integridad como la disponibilidad de los datos.[6]

3.3. Protocolo de comunicación y consenso

Ahora bien, cuando algún usuario externo emite alguna nueva transacción, el conjunto de nodos que componen la blockchain, se intercomunican para intentar validar la transacción, y en dicho caso almacenarla en la blockchain (en todas las replicas, por supuesto). Para validar la transacción,

6 https://en.wikipedia.org/wiki/Information_security. Accedido el 25/05/2019.

cada nodo tiene que resolver una especie de puzzle, un problema matemático difícil (calcular un hash criptográfico con unas condiciones determinadas: ser menor a un valor específico, es decir, empezar con un determinado número de ceros). Este problema es probabilísticamente imposible de resolver de otra forma que no sea con fuerza bruta. Así, cuando algún nodo lo resuelve, esta resolución es prueba suficiente de que dicha computadora estuvo haciendo muchísimos cálculos mientras el resto de los nodos también lo hacían. Y verificar la resolución es una tarea simple, así que el resto de los nodos pueden comprobar que en efecto la resolución es válida, y por ende también la transacción.

Todo este proceso, involucra un consumo eléctrico enorme, y a la vez es bastante lento[8]. En la actualidad, existen diversas ideas de algoritmos alternativos con los cuales construir los protocolos de consenso (todos basados en lo que se conoce como el problema de los *generales bizantinos* (Lamport, Shostak, Pease, 1982), que busca que un conjunto de principales se pongan de acuerdo aún sin confiar unos en otros). Realizando esto, se podrá lograr que la blockchain sea mucho más escalable, y pueda realmente trascender.

4. El ecosistema actual

Ya mencionamos que los conceptos de blockchain recién discutidos nacieron con la aplicación bitcoin. También dijimos que existen muchas otras aplicaciones por sobre esta tecnología. La tecnología en sí sigue básicamente los conceptos técnicos recién mencionados, pero cada aplicación puede implementar diversas variantes de dichos conceptos. Existe una blockchain en particular, conocida como *Ethereum* (Buterin, 2013), que implementa una *máquina virtual*[7] por sobre la infraestructura, y con esto permite desarrollos personalizados.

4.1. Contratos inteligentes

Como dijimos, la blockchain denominada Ethereum tiene la característica principal de implementar una máquina virtual (llamada EVM, por Ethereum Virtual Machine). Además, y gracias a esta máquina virtual, es posible correr cualquier aplicación por encima. Esta es una gran diferencia con otras blockchains como la de bitcoin, que es lo que se conoce como "de aplicación específica" (porque toda la blockchain está dedicada a una aplicación determinada, en este caso la aplicación bitcoin).

En cambio, en la EVM de cada nodo de Ethereum corre un lenguaje *Turing-completo* (Preukschat, 2017), es decir un lenguaje de programación que permite realizar cualquier operación que pueda ser programada. Así, con este lenguaje se pueden hacer programas, y escribir cualquier aplicación. Esto programas son conocidos como *contratos inteligentes*.[8]

Debido a esto, hay un ecosistema compuesto de diversos *stakeholders*,[9] los cuales son todos fuertes:

» Desarrolladores "de la VM". Estos son los desarrolladores que crean el software base para llevar adelante el consenso, además de realizar cualquier nueva propuesta para las estructuras de datos, algoritmos, y/o mejorar la infraestructura en general.

7 https://es.wikipedia.org/wiki/M%C3%A1quina_virtual. Accedido el 25/05/2019.
8 https://es.wikipedia.org/wiki/Contrato_inteligente. Accedido el 25/05/2019.
9 https://es.wikipedia.org/wiki/Parte_interesada_(empresas). Accedido el 25/05/2019.

» Desarrolladores de "contratos". Estos son los que crean el software "de aplicación", es decir cualquier tipo de aplicación que pueda correr por sobre Ethereum.
» Nodos (conocidos como *mineros* en algunas blockchains, por ejemplo en bitcoin). Son las computadores físicas que realizan los consensos y validan transacciones (para ser precisos, los stakeholders serían sus dueños o administradores).
» Inversores. Son personas que pueden poner dinero como "resguardo de valor", ya que tienen la expectativa de que la blockchain sea cada vez más usada y sus tokens asociados aceptados como bien de cambio. También pueden aportar su dinero para que otros puedan crear aplicaciones y, en caso de la aplicación prosperar, tener alguna ventaja competitiva en cuanto a su uso. Todo esto hace que los precios suban.
» Usuarios de contratos. Son los que lanzan transacciones externas a ser realizadas en la blockchain. Con esto le dan vida al sistema.
» Investigadores / innovadores. Con sus ideas, desarrollos y propuestas, hacen crecer la tecnología.

4.2. Aplicaciones existentes, en desarrollo y futuras

Según mencionamos previamente, se podría implementar con blockchain cualquier aplicación que incluya transacciones que deban ser almacenadas con seguridad casi absoluta. Una aplicación evidente para esto está relacionada al tema de transacciones inmobiliarias. Así, una escritura podría ser almacenada en la blockchain. Tanto en Suecia como en Dubai, existen proyectos para crear aplicaciones en blockchain para lograr esto (Zuckerman, 2018; Hochstein, 2017).

Cambiando completamente de rubro, y pensando en el mundo de los videojuegos, sabemos que existen diversos juegos en donde los jugadores tienen algún objeto, animal o personaje, y que lo pueden ir adaptando, mejorando, entrenando, etc. Para esto, los jugadores invierten tanto tiempo como posiblemente dinero. Si alguna vez el servidor del juego es apagado, o incluso hackeado, un jugador puede perder toda su inversión. Existe un juego basado en blockchain llamado *CryptoKitties*,[10] el cual ya está implementado y es una realidad. En este juego, el jugador puede comprar gatos, darles de comer, aparearlos, con esto generar otros gatos, e incluso venderlos. Algo muy peculiar ocurrió un tiempo atrás: hubo un caso de alguien que vendió su cryptokitty al precio de USD170 mil. Se podría llegar a pensar que esto es una locura, pero también tenemos que considerar que el comprador quizá tuvo la visión de que en el futuro, quizá 5 años, quizá 10, todo el mundo va a jugar al juego, y este va a ser un gato famoso por haber sido el primero que se vende por un precio exorbitante, y al ser tan famoso podría valer muchísimo más.

Por último, mencionamos un caso en el cual el autor del presente artículo estuvo involucrado. Existe un club de fútbol, cuyo equipo masculino milita en la Primera D de AFA, llamado Atlas.[11] Este club se hizo famoso gracias a un reality show en el cual se mostraban los entrenamientos, sus hinchas, y demás interioridades del equipo, que al público le parecía interesante.[12] El equipo femenino de este club, tiene la particularidad de que cada jugadora tiene un sponsor diferente. Con esto, y teniendo en cuenta que para el sponsor no da lo mismo que la jugadora que sponsorea juegue a que vaya al banco, se nos ocurrió la idea de poder registrar las apariciones de cada jugadora en la blockchain. La arquitectura de la aplicación distribuida completa, consta de la parte de blockchain en donde se registran las apariciones,

10 https://www.cryptokitties.co/. Accedido el 25/05/2019.
11 https://es.wikipedia.org/wiki/Club_Atl%C3%A9tico_Atlas. Accedido el 25/05/2019.
12 https://es.wikipedia.org/wiki/Atlas,_la_otra_pasi%C3%B3n. Accedido el 25/05/2019.

así como también de un servidor que manipula los datos y se conecta con la blockchain, y también un frontend para que el usuario interactúe. Este frontend está implementado en *Telegram*,[13] y es fácilmente utilizable mediante un *bot*.[14]

5. Conclusiones

En el presente artículo, realizamos un análisis superficial de diversas cuestiones relacionadas con la tecnología blockchain. Comenzamos con cuestiones conceptuales sobre blockchain, su funcionamiento y su uso, pasamos por algunas cuestiones técnicas, y luego nos focalizamos en algunas aplicaciones representativas. Como corolario, podemos mencionar que existen más de mil *startups* relacionadas al mundo blockchain, y esto evidencia el gran interés mundial por esta tecnología.

Bibliografía

» Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". Disponible en bitcoin.org.

» infotechnology.com (12/8/2016). ¿Qué es blockchain, la tecnología que viene a revolucionar las finanzas? https://www.infotechnology.com/online/Que-es-blockchain-la-tecnologia-que-viene-a-revolucionar-las-finanzas-20160810-0001.html. Accedido el 25/05/2019.

» unocero.com (25/1/2019). WhatsApp ya superó a Facebook como la app más usada del mundo https://www.unocero.com/software/apps/whatsapp-supera-facebook/. Accedido el 25/05/2019.

» Yahya, A., Chen, F. (2019). Five open problems for the Blockchain Computer. *A16z.com* https://a16z.com/2019/04/19/five-open-problems-blockchain-computer/. Accedido el 25/05/2019.

» medium.com (2018). What is a Dapp? https://medium.com/hbus-official/what-is-a-dapp-eec896a4bbbf. Accedido el 25/05/2019.

» Bass, L., Clements, P., Kazman, R. (2012). *Software Architecture in Practice*. New Jersey: Addison-Wesley Professional.

» Lamport, L., Shostak, R., Pease, M. (1982). The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.* vol. 4, num. 3.

» Buterin, V. (2013). "Ethereum White Paper: A next-generation smart contract and decentralized application platform". Accesible desde https://github.com/ethereum/wiki/wiki/%5BSpanish%5D-White-Paper.md

» Preukschat, A. (2017). Ethereum es Turing completo ¿y eso qué es? www.eleconomista.es https://www.eleconomista.es/economia/noticias/8817210/12/17/Ethereum-es-Turing-completo-y-eso-que-es.html. Accedido el 25/05/2019.

» Zuckerman, M. J. (2018). Swedish Government Land Registry soon to conduct first Blockchain Property Transaction. https://cointelegraph.com/news/swedish-government-land-registry-soon-to-conduct-first-blockchain-property-transaction. Accedido el 25/05/2019.

» Hochstein, M. (2017). Dubai Land Department launches Blockchain Real Estate Initiative. https://www.coindesk.com/dubai-land-department-launches-blockchain-real-estate-initiative. Accedido el 25/05/2019.

13 https://web.telegram.org/#/login. Accedido el 25/05/2019.
14 https://en.wikipedia.org/wiki/Internet_bot. Accedido el 25/05/2019.