ARTÍCULO ACEPTADO

La adopción del Blockchain por la nueva era digital como un sistema descentralizado para el uso y creación de nuevos servicios digitales

Fernando Rebollar Castelan, Marco Antonio Ramos Corchado y Rosa María Valdovinos Rosas

La comunidad de ingenieros de todo el mundo han aplicado su creatividad para construir máquinas y sistemas que han permitido automatizar y eficientizar numerosos procesos y servicios. La tendencia para continuar por el mismo camino es mantener conectados la mayor cantidad de dispositivos electrónicos a la red, los cuales son dotados de mayor funcionalidad con respecto a su estado anterior. En la era digital han surgido empresas que fungen como intermediarias de varios servicios, con la información obtenida de sus usuarios han lucrado ampliamente. Hoy día están surgiendo tecnologías descentralizadas como el Blockchain que dará un giro a los servicios digitales al permitir eliminar los intermediarios. Por otra parte, el Blockchain mediante los smart contracts permitirá automatizar servicios que antes no eran posibles, como programar un auto para que compre su combustible o permitir que una celda solar venda la energía que produzca, entre muchas otras aplicaciones que surgirán en la nueva era digital.

Introducción

Desde hace varias décadas, la búsqueda de mecanismos que permitan automatizar y hacer eficientes los procesos de producción, han sido una constante. Con el crecimiento exponencial de la tecnología, máquinas, robots y diversos sistemas son de fácil identificación en múltiples cadenas de producción de bienes y servicios. Ahora, la tendencia es aumentar la funcionalidad de estos dispositivos electrónicos, al agregarles la capacidad de interconectarse a la red.

Tal y como sucedió con los celulares que se convirtieron en celulares inteligentes, después las televisiones pasaron a ser televisiones inteligentes, lo mismo está ocurriendo con los autos y se espera que la mayoría de los aparatos electrónicos y mecánicos evolucionen en la misma línea. A toda esta nueva funcionalidad de los dispositivos, que requieren permanecer conectados a la red se le denominan *Internet de las cosas* (IoT por *Internet of Things* en inglés).

El conjunto de estos dispositivos intercambiando información en determinadas zonas ha permitido generar conceptos como casas, oficinas y edificios inteligentes, incluso ya se habla de ciudades inteligentes, las cuales estarán dotadas de una diversidad de dispositivos interconectados repartidos por todas partes, por ejemplo semáforos, señales de tránsito, puentes peatonales, cámaras públicas, etc. Toda información que se genere necesitará ser propagada por la red de manera segura para garantizar que sea completa, objetiva, confiable y confidencial. Se ha estimado que todos estos dispositivos interconectados generarán grandes cantidades de información en tiempo real (no todos confiables), y con frecuencia tendrán implicaciones de privacidad y seguridad [1]. Esta situación ha sido de creciente interés para algunos proveedores que han obtenido importantes ganancias como el uso del teléfono celular y la información tan codiciada por distintas organizaciones. Por ejemplo, el fabricante del celular o el creador de su sistema operativo (por ejemplo Google en android) donde suelen preguntar al usuario de dicho dispositivo si desea enviar datos de uso "anónimo". En este sentido, empresas como Google y Facebook, entre otras, han logrado monetizar toda la información que obtienen por medio de sus usuarios, actuando como intermediarios entre personas, empresas y anunciantes. Otro ejemplo de esto es Amazon, eBay y Mercadolibre entre otras, las cuales conectan compradores con vendedores. Uber conecta a personas con la necesidad de transportarse de un lugar a otro con personas con vehículos que pueden llevarlos. Airbnb conecta anfitriones con huéspedes.

La existencia de los intermediarios no es algo nuevo, los sistemas financieros digitales hacen uso de los bancos para que actúen como intermediarios entre los negocios y clientes, obteniendo información de ambas partes con la cual se benefician.

La nueva era digital busca eliminar la participación de intermediarios que validan la información y mediante la llegada del *Blockchain*, es probable que la información logre descentralizarse siendo esta posibilidad el tema central del presente artículo.

La descentralización en la nueva era digital

La nueva era digital ahora está buscando eliminar a todo tipo de intermediarios, con el objetivo de conectar a las personas, empresas, organizaciones, etc. sin que una tercera parte esté involucrada en los procesos.

La pregunta es ¿Esto puede ser posible? Dado que el intermediario mantiene un control de los datos que están siendo transferidos digitalmente y evita o al menos trata de prevenir numerosos tipos de fraudes. La respuesta

© 2020 - Sociedad Mexicana de Inteligencia Artificial ISSN 2007-0691

está en analizar lo que pasa en la realidad dejando fuera todos los sistemas digitales; cuando se compra un producto o servicio, el cliente entrega el dinero a cambio del producto o servicio, en cambio el proveedor ofrece el producto o servicio y recibe dinero. Durante la transacción se mantiene el anonimato puesto que ni el cliente ni el proveedor necesitan conocerse para realizar la transacción; por otra parte no existió la necesidad de que una tercera persona tuviera que revisar la operación para declarar que fue legitima, por lo que se dice que es una transacción descentralizada y anónima. En cambio al realizar la compra por un medio digital (por ejemplo pagar con tarjeta de débito), es necesario que el banco se involucre en la transacción puesto que debe verificar que el cliente tenga el suficiente dinero digital para cubrir los costos y después debe conocer al proveedor para entregar el dinero de su venta. La transacción no es anónima y está centralizada en el sistema bancario.

La nueva era digital busca eliminar a intermediarios en las transacciones digitales mediante la descentralización de la información. Existe desconcierto en el significado de la descentralización y es confundido con los sistemas distribuidos. Sin embargo, un sistema distribuido se refiere a una configuración arquitectónica de los equipos implicados en un mismo sistema. Justo en las palabras "en un mismo sistema" está la clave, puesto que se debe pensar a otro nivel para entender la diferencia entre descentralizado y distribuido. Según Buterin [2], "distribuido significa que no todo el procesamiento de las transacciones se hace en el mismo lugar, mientras que descentralizado significa que no hay una única entidad que tenga control sobre todo el procesamiento".

Algunos de los tipos de sistemas descentralizados son:

Descentralización arquitectónica: Se refiere a los equipos físicos que dan un determinado servicio y manejan protocolos que en caso de fallas controlan cuantas computadoras se puede permitir el sistema perder, sin que el mismo sistema se colapse.

Descentralización política: Se refiere al número de individuos y/o organizaciones que controlan los equipos de los que se conforma el sistema.

Descentralización lógica: Se refiere a un sistema que si fuese cortado a la mitad, él mismo podría funcionar como dos partes completamente funcionales.

Hasta ahora el Internet es el único sistema que cumple con los tres tipos de descentralización, ya que está compuesto de un gran número de computadoras físicas distribuidas por todo el mundo, no la controla una organización, individuo o gobierno, de tal forma que si se eliminaran conexiones entre continentes enteros éstas seguirán funcionando. La descentralización política es a la que se hace referencia en este artículo cuando se menciona la eliminación de intermediarios, es decir que ninguna organización sea la que tenga el control del sistema. Era difícil imaginar un servicio digital confiable en el que ninguna organización validara la información del mismo sistema y que fuera lo suficientemente seguro para resistir ataques, hasta que apareció el *Blockchain*.

Blockchain

El 31 de octubre del 2008, Satoshi Nakamoto publicó el artículo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" [3] en un foro de criptografía. En su artículo propuso un sistema distribuido y políticamente descentralizado para un sistema de envió de dinero mediante tokens digitales, que utilizado un conjunto de técnicas criptográficas, es capaz de validar las transacciones entre los usuarios a través de los mismos nodos de la red que se conectan voluntariamente. El 3 de enero del 2009 fue generado el primer token y así fue como nació el Bitcoin (nombre que se le dio al token) y a la tecnología distribuida se le nombró *Blockchain* (la traducción popular al español es cadena de bloques), debido a que cada determinado tiempo generaba un bloque sellado criptográficamente que era unido a un bloque anterior [4].

A. Funcionamiento general del Blockchain

Para explicar el funcionamiento del *Blockchain* es importante mencionar algunos conceptos clave que brevemente se explican a continuación.

Hash: Es una huella digital de un archivo que tiene una determinada estructura y de tamaño fijo. Sin importar el archivo de entrada siempre el resultado es del mismo tamaño, una de sus características es ser irreversible, es decir a partir de un *Hash* es imposible calcular el archivo del cual se obtuvo. Otro atributo es que con cualquier cambio en el archivo, por mínimo que este sea, el *Hash* de salida cambia completamente. Un ejemplo de algoritmo *Hash* es SHA256.

Proof-of-work: Es una técnica similar al *Hashcash* propuesta inicialmente por Adam Back [5], para combatir el *spam* en los correos electrónicos. Consiste en generar una prueba de trabajo de cómputo obligando al *Hash* de un archivo a iniciar con varios ceros en sus cadenas de bits, a mayor número de ceros iniciales en el *Hash* mayor la dificultad para encontrar el *Hash* válido, por lo que mayor es la prueba de trabajo necesaria.

Nonce: Es un número que se agrega al contenido de un archivo, el *nonce* se utiliza para variar el contenido del archivo hasta encontrar un *Hash* que satisfaga la *proof-of-work* de mismo archivo [3].

Con estos mínimos conceptos se puede explicar el funcionamiento general del *Blockchain* de la siguiente manera: en un bloque se agrega la información que se desea guardar, dentro del mismo bloque se agrega el *Hash* del bloque anterior que debe cumplir con las características

© 2020 - Sociedad Mexicana de Inteligencia Artificial ISSN 2007-0691

de la *proof-of-work*, también se agrega el número *Nonce* que será necesario variar para cuando se calcule el *Hash* del bloque. Cada determinado tiempo el bloque se sella con la *proof-of-work* (a esto se le conoce como minado de bloques) y se crea el siguiente bloque. Cualquier cambio en un bloque ya sellado por mínimo que sea cambiará completamente su *Hash* y se volverá un bloque inválido así como todos los bloques que aparezcan después del mismo al que se le modificó la información. En la Figura 1 se ilustran los datos esenciales que se incluyen en cada bloque y cómo el siguiente bloque contiene el *Hash* del previo.

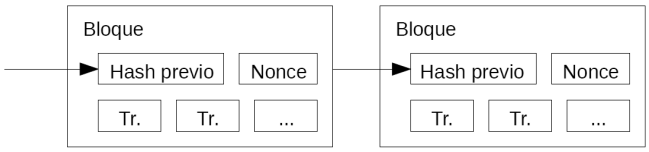

Figura 1. Bloques con los datos generales del *Blockchain* [3].

Esta serie de bloques se copian en diferentes computadoras haciendo una descentralización física y por medio de algoritmos de consenso se sincronizan y actualizan. Si es un *Blockchain* público cualquier computadora se puede unir a la red, si es un *Blockchain* privado solo se pueden unir determinadas computadoras autorizadas. Más adelante se explicará ésto. El sellado criptográfico dificulta a posibles atacantes modificar la información de los bloques e impiden que estos se distribuyan en la red como bloques válidos [4].

B. Implementaciones del Blockchain

A medida que se popularizó el Bitcoin, surgieron varias versiones con modificaciones a la versión implementada en el Bitcoin (la primera implementación registrada del *Blockchain*), con mejoras en la implementación y funcionalidad del *Blockchain*. Con esto surgieron nuevos tokens con distintas versiones de mejoras a la tecnología *Blockchain*. Existen dos implementaciones principales del *Blockchain* una pública y otra privada.

1. *Blockchain pública.* Permite que cualquier computadora se pueda unir a la red, son políticamente descentralizadas puesto que el control pertenece a la misma red y por lo mismo requieren de la máxima seguridad para impedir que alguna organización o individuo tome el control de la red, a mayor distribución de la red mayor es su dificultad para realizar un ataque. Para lograrlo sacrifican velocidad en las transacciones que se pueden almacenar en el bloque. Algunos ejemplos de *Blockchain* púbicas son Bitcoin [3] y Ethereum [6]. Ethereum, genera tokens llamados ETH e implementa una mejora para agregar funcionalidad que permite utilizar *smart contracts* (programas que ejecutan acuerdos registrados entre dos o más entes), capaces de ejecutarse cuando se cumplan las condiciones del contrato, la tecnología de *Blockchain* comprueba automáticamente el cumplimiento de dichas especificaciones con un alto grado de confiabilidad [6].

2. *Blockchain privada.* Estas *Blockchain* no permiten que cualquier computadora pueda realizar las verificaciones de su red, normalmente pertenecen a empresas u organizaciones que las controlan, algunas permiten el acceso al contenido de sus bloques, otras no, por ejemplo la empresa Ripple realizó su implementación produciendo su token XRP que redujo la cantidad de tiempo necesario para que se confirmara una transacción (segundos) [7]. Esto le impide ser políticamente descentralizada, la seguridad recae en la empresa, pero su principal ventaja es que puede validar transacciones más rápido que una *Blockchain* pública.

A estos tokens funcionando en sus propios *Blockchains* pronto se le agregaron más y ahora se les conoce como criptomonedas. Pero el *Blockchain* no solo puede ser implementado en las criptomonedas, también puede emplearse en diversos casos de uso. Por ejemplo, Zyskind et. al. [8] presentaron una propuesta donde utilizaban el *Blockchain* para la protección de datos personales y confidenciales, encriptando el contenido que se guardaba en el bloque.

Otro uso propuesto es el sistema de votos basado en *Blockchain* [9], en el que una vez emitido el voto es imposible de cambiar y permite realizar el conteo de votantes y votados con total seguridad, evitando la posibilidad de fraudes, ya que si alguien trata de cambiar uno o varios votos emitidos el bloque se convierte en un bloque invalido. Este mismo enfoque se puede utilizar para registrar certificados, cédulas, identificaciones y demás documentos que suelen ser susceptibles a falsificaciones, donde los válidos son registrados en un bloque con fecha fija y los falsos de ninguna manera se pueden agregar a una fecha ya pasada.

La criptografía mantiene la integridad de la información sin la necesidad de que organizaciones la validen

© 2020 - Sociedad Mexicana de Inteligencia Artificial ISSN 2007-0691

C. Retos del Blockchain

J. Leon et. al. [10] plantean que el "*Blockchain* está a punto de convertirse en la invención más emocionante después de Internet", sin embargo, destacan que la tecnología *Blockchain* todavía se encuentra en una etapa de desarrollo y se necesita realizar más investigación para mejorar su eficiencia y seguridad. Además advierten que los investigadores se enfrentan a oportunidades y desafíos para hacer que el *Blockchain* sea exitoso, debido a sus distintas desventajas que se mencionan a continuación:

- En caso de que se quiera distribuir indiferentemente los nodos que comprueban las transacciones, necesitan ser recompensados por el mismo trabajo criptográfico que realizan (los llamados mineros), lo que genera un coste por transacción el cual aumenta conforme aumenta la demanda de transacciones.
- Dado que el *Blockchain* requiere un proceso de verificación muy estricto para crear un nuevo registro de transacciones, cuando se supera la capacidad de comprobación de transacciones, surge una cola de transacciones a confirmarse. Lo anterior vuelve lento el proceso de confirmaciones y hace que se presente un desperdicio de recursos computacionales porque distintos equipos trabajan para generar el siguiente bloque en la cadena pero solo uno (el que termina primero) lo agrega. Es decir presenta problemas de escalabilidad.
- Un problema en los *Blockchain* públicos surge cuando no existe la suficiente distribución en el *Blockchain* ya que si un nodo concentra el 51 % (más de la mitad) de poder de procesamiento puede dominar a todos los demás nodos y manipular los registros en una cadena de bloques. Pero solo podrían manipular los últimos bloques de la cadena ya que entre más antiguo es el bloque mayor cantidad de procesamiento se requiere.
- La privacidad y la confidencialidad siguen siendo un problema con el *Blockchain*, debido a que todos los nodos de la cadena de bloques tienen acceso a todos los datos, aunque no puedan modificarlos, esto también depende de la aplicación que se le quiera dar.

Debido a estos problemas surgen nichos de oportunidad de mejora.

Para mejorar la escalabilidad en el *Blockchain* han surgido diversas propuestas de distintos grados de modificación al *Blockchain* original. Los primeros buscaban resolver el problema sin modificar el funcionamiento del *Blockchain*, aumentando el tamaño del bloque un determinado porcentaje. No obstante el problema se solucionaba momentáneamente, después se propuso eliminar el límite del tamaño de bloque pero eso generaría bloques de gran tamaño y solo empresas con grandes cantidades de almacenamiento podrían ser mineros, lo que haría que se centralizara la red *Blockchain*. Existen otras modificaciones similares a las mencionadas y en general se observan entre una y otra que se pueden obtener dos de los siguientes tres atributos [10]: seguridad, descentralización, velocidad de transacciones, como se puede ver en la Figura 2.

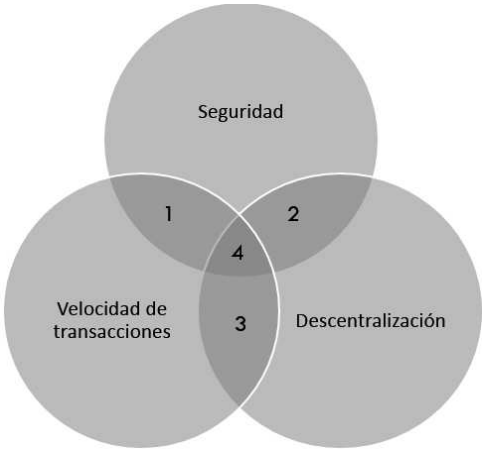

Figura 2. Atributos de los *Blockchains*.

De acuerdo a la Figura 2 se tienen cuatro opciones:

1. Se configura el *Blockchain* para aumentar la velocidad de transacciones y se mantenga seguro. La desventaja es que se termina centralizando la red, hasta ahora son controladas por organizaciones, es común en los *Blockchain* privados.
2. Aumentar la velocidad de transacciones y estar descentralizada. Esta opción implica bajar la seguridad, siendo la opción menos recomendada puesto que la seguridad es prioritaria.
3. Se configuran para estar descentralizadas y mantener la seguridad en la red, sacrifican la velocidad en las transacciones, es común en los *Blockchain* públicos.
4. Es el estado ideal donde se obtienen los tres atributos deseables, seguridad, velocidad de transacciones y descentralización.

Conclusiones

El *Blockchain* ha demostrado tener la suficiente capacidad criptográfica para ser confiable, su utilización sigue en constante aumento, las aplicaciones para las que puede ser utilizado están aumentando conforme distintos grupos de usuarios lo conocen. En algunos años gobiernos, organizaciones públicas y privadas utilizarán directa o indirectamente sistemas basados en *Blockchain* por lo que será importante contar con personas calificadas para

© 2020 - Sociedad Mexicana de Inteligencia Artificial ISSN 2007-0691

implementar el uso de estos sistemas, gobiernos y universidades deberán invertir en la generación de personal capacitado. En cuanto sea viable van a desaparecer algunos intermediarios de servicios que puedan ser sustituidos por los *smart contracts* que funcionan en distintos *Blockchain* por lo mismo se requiere más investigación para ambos. Los *Blockchain* públicos son difíciles de regular por los gobiernos, por lo que corren el riesgo de ser prohibidos o limitados en varios países. Sin embargo, los propios gobiernos seguramente implementaran sus propios *Blockchain* para montar uno o varios de sus servicios actuales. También es probable que los países emitan su propia criptomoneda en un futuro, como es el caso de Venezuela que ya ha emitido la suya. Finalmente habrá que estar pendientes de los cambios y novedades de estas tecnologías para intentar prever lo que se aproxima en un futuro no muy lejano. ✷

REFERENCIAS

1. Maged N., Boulos k. y Najeeb M. Al-Shorbaji. (2014) "On the internet of things, smart cities and the who healthy cities". International journal of health geographics, Vol. 13, pp 5-7.
2. Vitalik Buterin. (2017) "The Meaning of Decentralization". Recuperado el 7 de noviembre de 2018, de https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
3. Satoshi nakamoto. (2008) "Bitcoin: A Peer to Peer Electronic Cash System". Recuperado el 7 de noviembre de 2018, de https://bitcoin.org/bitcoin.pdf
4. Melanie Swan. (2015) "Blockchain: Blueprint for a new economy". O'Reilly Media.
5. Back, A. (2002) "Hashcash-a denial of service countermeasure". Recuperado el 7 de noviembre de 2018, de https://gnunet.org/sites/default/files/hashcash.pdf
6. Vitalik Buterin. (2014) "A next-generation smart contract and decentralized application platform". Recuperado el 7 de noviembre de 2018, de https://github.com/ethereum/wiki/wiki/White-Paper
7. Noah Schwartz, David S. y Arthur Britto. (2014) "The ripple protocol consensus algorithm". Ripple Labs Inc, White Paper. Vol 1, pp 5-6.
8. G. Zyskind, O. Nathan and A. (2015) "Decentralizing privacy: Using blockchain to protect personal data". En 2015 IEEE Security and Privacy Workshops, San Jose, pp 180-184.
9. Yehuda Lindell. (2011) "Highly-efficient universally-composable commitments based on the ddh assumption". En Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp 446-466.
10. J. Leon Zhao, Shaokun Fan y Jiaqi Yan. (2016) "Overview of business innovations and research opportunities in blockchain and introduction to the special issue". Financ Innov. Vol. 2 Springer, pp 3-7.

SOBRE LOS AUTORES

Fernando Rebollar Castelan Maestro en Ciencias de la Ingeniería y estudiante del Doctorado en Ciencias de la Ingeniería, que se imparte en la Facultad de Ingeniería de la Universidad Autónoma del Estado de México. Los intereses de investigación son sobre computo paralelo, sistemas multiagentes, sistemas distribuidos y ahora entusiasta del Blockchain y de nuevas tecnologías que permitan revolucionar los servicios digitales.

Marco Antonio Ramos Corchado Profesor investigador en Inteligencia Artificial y Realidad Virtual en la Universidad Autónoma del Estado de México y miembro del Sistema Nacional de Investigadores SNI. Obtuvo su doctorado en la Universidad de Toulouse en 2007, Francia. Sus temas de investigación son: Vida Artificial, técnicas de animación, sistemas distribuidos, agentes inteligentes, etc.

Rosa María Valdovinos Rosas Doctora en Ciencias Computacionales, miembro del Sistema Nacional de Investigadores SNI Nivel I, del Registro CONACYT de Evaluadores Acreditados y del PRODEP. Miembro activo de la Asociación Mexicana de Inteligencia Artificial, de la Red Mexicana de Investigación y Desarrollo en Computación y de la Academia Mexicana de Computación. Los intereses en investigación son: Sistemas de Múltiple Clasificación, Algoritmos Genéticos, Redes Neuronales Artificiales, Reconocimiento de Patrones y minería de datos.

© 2020 - Sociedad Mexicana de Inteligencia Artificial ISSN 2007-0691