

Trazabilidad con Blockchain

Manuela Linares Barbero
malinare@ulima.edu.pe / Universidad de Lima. Lima, Perú

Recepción: 13-7-2018 / Aceptación: 8-8-2018

RESUMEN. En la actualidad los consumidores muestran mayor preocupación por conocer la procedencia de los productos que adquieren y procuran informarse mejor sobre estos. Tal situación obliga a las empresas no solo a ofrecer información bastante completa a los consumidores finales, ya sean personas naturales o instituciones, sino que deben preocuparse por obtener dicho conocimiento de sus proveedores y de los proveedores de insumos de sus proveedores, es decir, de toda la cadena de suministro. Hoy se empiezan a observar algunas propuestas para solucionar este problema de trazabilidad empleando la tecnología Blockchain, que ha captado la atención tanto de empresarios como de académicos. En nuestro artículo nos enfocaremos en la aplicación de la plataforma de Blockchain en la cadena de suministro, en función de los beneficios que propone la trazabilidad.

PALABRAS CLAVE: Blockchain, cadena de suministro, trazabilidad, sistemas distribuidos

Traceability with blockchain

ABSTRACT. Currently, consumers are more concerned about the origin of the products they buy and seek to learn more about them. This situation forces companies not only to offer complete information to final consumers, whether they are individuals or institutions, but also to be concerned about obtaining this knowledge from their suppliers, and suppliers of supplies for their suppliers, that is, of the entire supply chain. Today we begin to observe some proposals to solve this problem of traceability using the Blockchain technology, which has attracted the attention of both executives and academics. In our article, we will focus on the application of the Blockchain platform in the supply chain, based on the benefits proposed by traceability.

KEYWORDS: Blockchain, supply-chain, traceability, distribute system

1. INTRODUCCIÓN

La globalización del comercio ha facilitado a los consumidores la compra de bienes de diferentes partes del mundo en tiendas o supermercados locales. Un consumidor puede adquirir objetos de marcas extranjeras, como zapatillas de los Estados Unidos, y detecta que el país de producción es otro como, por ejemplo, China. Por eso, es necesario observar detalladamente la mercancía con la finalidad de descubrir su procedencia real. Si analizamos productos de orden alimenticio el fenómeno se acentúa. Ello nos demuestra la importancia de poder contemplar la trazabilidad de cada artículo e ir más atrás: no solo donde se ha generado el bien, sino también donde se originaron sus insumos. El presente trabajo busca detallar el beneficio de trazabilidad que nos ofrece Blockchain en la cadena de suministro.

La tecnología Blockchain nos permite identificar la trazabilidad de cada producto y de cada insumo al generar un registro inalterable de tiempos en cada etapa del producto o insumo. La generación de un registro de fabricación del producto no es algo nuevo, sin embargo, la difusión del registro se limita a cada empresa. La nueva tecnología Blockchain, en su forma privada, posibilita recurrir a un registro desde los insumos originales hasta el consumidor final e incluso hasta el mercado de segunda mano. Así, por ejemplo, se puede averiguar qué tipo de alimento consumió la vaca cuyo cuero sirvió para fabricar una determinada cartera.

2. BLOCKCHAIN

El trabajo colaborativo no es un concepto nuevo; se ha utilizado en diversas áreas del conocimiento con éxito. Dicho concepto ha pasado paulatinamente a la ciencia de la computación en la forma de sistemas distribuidos, que se han empleado en diferentes niveles por varios años. Motivados por nuevos retos se desarrollan conceptos y tecnologías como es la de Blockchain que recientemente ha llamado la atención de la academia y del mundo empresarial.

La tecnología Blockchain busca efectuar transacciones descentralizadas entre entidades sin la necesidad de que prime la confianza entre estas. La plataforma en mención pretende eliminar la entidad que centraliza la información, así como la autorización de las transacciones. De esta forma se elimina la redundancia de procesos y también la necesidad de una entidad intermediaria, ya que el público en la red puede observar la transacción. Se estima un ahorro de 6 billones de dólares en el mercado actual de capitales al eliminar el doble esfuerzo en el gobierno de los datos (Goldman Sachs Group, 2016). Y se proyecta para el 2020 que la tecnología de Blockchain ayudará a eliminar los procesos duplicados antes mencionados (Morgan y Wyman, 2016).

La Blockchain más famosa es Bitcoin, criptomoneda creada con el propósito de resolver el problema de doble gasto en las transacciones (Christidis y Devetsikiotis, 2016). No obstante, en la actualidad no es la única Blockchain que nos facilita esta forma de dinero. Podemos

clasificar a las Blockchain de acuerdo con las funciones que nos ofrecen. Esta propiedad se clasifica en tres tipos: las que nos presentan una criptomoneda, como indicamos; las que digitalizan activos o bienes, es decir, permiten el seguimiento del valor y el dueño de un activo o bien, y finalmente las que nos extienden una mayor gama de procesos para diferentes aplicaciones (Anh Dinh, Liu, Zhang, Chen, Chin Ooi y Wang, 2018). Para lograr las funcionalidades mencionadas debemos identificar la necesidad de una Blockchain pública, como Bitcoin, o privada, como Hyperledger Fabric. La diferencia radica principalmente en que la red pública les posibilita a todos los nodos el acceso y eventualmente la creación de nuevos bloques. Sin embargo, en la red privada existe una lista predefinida de los nodos que pertenecen a ella, y cada uno de estos presenta diferentes accesos.

En la Blockchain pública, con un mecanismo de consenso tradicional, todo aquel que posea un nodo tiene acceso a votar para validar una transacción o no, cada uno de estos cuenta con un solo voto. Ello trae consigo el ataque Sybil, que es cuando un nodo de forma maliciosa genera múltiples identidades para conectarse a la red y así contar con muchos votos y aprobar o rechazar una transacción de acuerdo a su conveniencia (Yeow, Gani, Rodrigues, Ahmad y Ko, 2017). Para mantener la integridad de la cadena de bloques y evitar estos ataques Sybil, se trabaja con el protocolo PoW (Proof-of-Work), con el que identificamos otra propiedad de Blockchain: el protocolo de consenso.

Existen varios protocolos de consenso. Los más utilizados son PoW, que se emplea con las Blockchain públicas y está basado netamente en cálculos computacionales para que un solo minero no pueda realizar más de un cálculo en simultáneo y así evitar el ataque Sybil (Anh Dinh *et al.*, 2018). Este protocolo utiliza los nodos de minería, los cuales pueden tener más de un minero, quienes son los que verifican las transacciones al encontrar el número *noncek* (número aleatorio) adecuado para el *hash* del contenido del bloque y el *hash* del bloque anterior, y recibe una recompensa en criptomoneda o algún *token* de la Blockchain. El nodo de minería seleccionado deberá realizar un algoritmo para formar el *hash* (SHA256) (Yeow *et al.*, 2017) y verificar así el bloque.

Nakamoto, creador de esta plataforma, en su versión original de Blockchain desarrolla el protocolo PoW, basado en los cálculos computacionales del CPU; luego pasó a la tarjeta de video del computador y el día de hoy al procesador ASIC (Application-Specific Integrated Circuit). Lamentablemente esto ha generado que más del 50 % del *hash power* se encuentre ubicado en China (Yeow *et al.*, 2017), más del 23 % de los nodos se encuentran ubicados en Estados Unidos y más de 18 % de los nodos se encuentran ubicados en Alemania (Yeow, 2018), lo que genera centralización.

Otro de los protocolos más comunes es el Practical Byzantine Fault Tolerance (PBFT), que se maneja con las Blockchains privadas y está basado principalmente en comunicación. En una red privada no es necesario usar recompensas porque todos los nodos de la Blockchain han sido predefinidos y no existe el riesgo de un ataque Sybil. Sin embargo, no se anula la probabilidad

de que alguno de sus nodos actúe de forma maliciosa o presente defectos. En este protocolo se acepta la transacción si dos tercios de los nodos la verifican. Por tanto, asume que los nodos maliciosos o defectuosos son menos de un tercio de los nodos de la red (Yeow *et al.*, 2017).

Debemos destacar que en la actualidad se cuenta con más de 17 plataformas de Blockchain con características diferentes (Shanley, 2017). Algunas públicas y otras privadas, una de las características más importantes es el protocolo de consenso, del que existe gran diversidad, pero estos han sido desarrollados basados en el PoW o PBFT ya mencionados, con algunas variantes buscando mejorarlos. Así, está el PoS (Proof of Stake), que intenta mejorar el PoW al reducir el trabajo de minado, minimizando el uso de energía eléctrica y adicionando un elemento de apuesta que puede estar definido como una función o un *smart contract*, como es en el caso de Ethereum con Casper (Anh Dinh *et al.*, 2018).

3. TRAZABILIDAD CON BLOCKCHAIN EN LA CADENA DE SUMINISTRO

La cadena de suministro constituye uno de los componentes más importantes en la empresa porque evita problemas de ruptura de *stock*, costos altos innecesarios, así como costos por robo o falsificación de productos, errores de planificación, entre otros. Por tal motivo múltiples soluciones han sido desarrolladas como modelos EDI (Electronic Data Interchange) para conectar proveedores, manufactureras y distribuidores, y así tener un mayor control de la planificación. También se utilizan modelos RFID (Radio Frequency IDentification) con la finalidad de evitar robos y falsificaciones de los bienes.

Sin embargo, estos modelos y muchos otros más están enfocados en la planificación de los órdenes de pedido y el almacenamiento de los bienes, e ignoran la trazabilidad de la cadena de suministro.

El beneficio que persigue la trazabilidad es que se pueda identificar claramente a los fabricantes de los productos, hasta el origen de los insumos. Recurriendo a la tecnología Blockchain se empiezan a desarrollar diferentes soluciones, como es el proyecto piloto de la cadena de tiendas Walmart Store Inc. con IBM, quienes en abril del 2017 iniciaron el desarrollo para fortalecer la cadena de suministro de alimentos y lograr la trazabilidad de la cadena de suministro *from-farm-to-table* (de la granja a la mesa), de mangos y carne de cerdo en China (Firica, 2017). Otra propuesta de aplicación de Blockchain es AgriBlockIoT, la cual utilizando IoT (Internet of Things o Internet de las Cosas) pretende conectar la cadena de suministro desde el productor hasta el consumidor final *from-farm-to-fork* (de la granja al tenedor) (Pincheira Caro, Salek Ali, Vecchio y Giaffreda, 2018).

La trazabilidad en la cadena de suministro ha cobrado gran importancia en la actualidad, no solo por la denominación de origen de los productos alimenticios, sino también para evitar

falsificaciones de insumos o de artículos de lujo, especialmente cuando estos últimos entran al mercado de segunda mano. Al analizar esta cadena de suministro reparamos en lo fácil que es para personas inescrupulosas alterar o copiar las etiquetas RFID que normalmente se usan para etiquetar los bienes.

Para realizar una trazabilidad precisa es necesario vincular el bien físico con el registro virtual, lo que se realiza con las etiquetas RFID o similares. El referido registro virtual se ejecuta en la plataforma Blockchain cuando un nodo minero genera el bloque, identificando la entidad, y lo ofrece a la red para su validación. En este punto se cuenta con varias soluciones de acuerdo con la ubicación en la cadena de suministro en la que se cree el registro. Así, por ejemplo, si un agricultor quiere registrar el crecimiento del cultivo o la venta de la cosecha, se puede usar un modelo con dispositivos como *smartphones*, tabletas, sensores, etcétera, para enviar la información y generar la transacción en el nodo minero más cercano, registrando así la transacción en la Blockchain (Pincheira Caro et al., 2018). En otro escenario, si un fabricante de aviones quiere verificar el aluminio usado en la turbina que está comprando de su proveedor, puede verificar esta información que se encuentra en la cadena de bloques (Madhwal y Panfilov, 2017). También, si un consumidor del mercado de segunda mano desea identificar la originalidad de una cartera de lujo, puede hacerlo verificando la fabricación del producto antes de realizar la compra (Toyoda, Sasase, Ohtsuki y Mathiopoulos, 2017). O un observador a través de un nodo monitor registra la transacción sobre la geolocalización de los bienes transportados para su seguimiento (Wu, Li, King, Miled, Wassick y Tazelaar, 2017).

Como mencionamos anteriormente, existen plataformas de Blockchain públicas en las cuales cualquier nodo podría generar un nuevo bloque, y plataformas de Blockchain privadas en las que todos los nodos son conocidos y cada uno tiene accesos específicos en cuanto a la creación y validación de bloques. Pensando en las diferentes transacciones no es difícil dar el siguiente paso y combinar soluciones que contemplen plataformas de Blockchain públicas y privadas. Al observar transacciones de transporte entre países, identificamos que entidades como aduanas u otras similares podrían beneficiarse de compartir la información en una Blockchain privada con cierta información pública y así facilitar el proceso (Engelenburg, Janssen y Klievink, 2017). Las transacciones de compraventa de moneda virtual o de valor de un bien físico también pueden beneficiarse con la Blockchain pública. Otras transacciones como el registro de producción o el manejo de inventarios pueden mantenerse en una Blockchain privada, especialmente si son bienes de valor o medicamentos. Es decir, las transacciones con los datos más sensibles es mejor retenerlas en una Blockchain privada, la que podría ser desarrollada con un modelo híbrido donde se combine la arquitectura física distribuida y de punto a punto, en la que se crea una subred por cada embarque de productos (Wu *et al.*, 2017). Evidenciamos así que es posible el desarrollo de múltiples modelos para cada solución particular.

Es importante destacar el papel de las plataformas de Blockchain. Al observar las pruebas realizadas comparando el desempeño de Ethereum y Hyperledger Saw-Tooth (Pincheira Caro

et al., 2018) o de Ethereum, Parity y Hyperledger Fabric (Anh Dinh *et al.*, 2018) en cuanto a número de transacciones y escalabilidad, podemos ver que a mayor escalabilidad menor número de transacciones, es decir menor velocidad. Esto nos demuestra que las Blockchain públicas como Bitcoin, que deben tener gran escalabilidad, se demoran 10 minutos por bloque (Anh Dinh *et al.*, 2018), y las Blockchain que ofrecen un gran rendimiento como Hyperledger Fabric v0.6.0 solo soportan ocho nodos. Nuevas versiones de Hyperledger Fabric v1.0 tienen mejor escalabilidad y menor rendimiento al utilizar el servicio centralizado Kafka (Anh Dinh *et al.*, 2018). La compensación entre escalabilidad y rendimiento mantiene las características primordiales de las plataformas Blockchain en cuanto a registro de tiempos, transacciones que no se pueden modificar o borrar y transparencia; todas son características que la trazabilidad puede ofrecernos.

4. CONCLUSIONES

Apreciamos la existencia de diferentes soluciones que se están investigando para lograr el gran beneficio que extiende la trazabilidad en la cadena de suministro. Cada solución se enfoca en una aplicación particular de la tecnología Blockchain. Esta nueva plataforma logrará cambios sustantivos como lo demuestran las tecnologías disruptivas. En el campo de la cadena de suministro, la tecnología de Blockchain nos permite evitar la falsificación de productos y ofrecer transparencia en la trazabilidad de los mismos. Sin embargo, se deben solucionar aún algunos problemas en cuanto al modelo, definir un diseño claro, detallar las pautas del gobierno de los datos y el modelo para aplicar incentivos, y, en cuanto a la implementación, determinar el rendimiento y la escalabilidad para que se convierta en algo real.

Se puede ver la compensación entre escalabilidad y rendimiento (cantidad de transacciones y tiempo de transacción). Algunas plataformas de Blockchain que ofrecen gran rendimiento solo soportan hasta ocho nodos, como Hyperledger Fabric v0.6.0 (Anh Dinh *et al.*, 2018); es difícil creer que la cantidad de nodos mencionada sea suficiente para una cadena de suministro conectada desde la generación de insumos hasta el consumidor final, peor aún si queremos pasar al mercado de segunda mano. Nuevas versiones de Hyperledger Fabric v1.0 tienen mejor escalabilidad, pero el rendimiento decrece. Otras demoran aproximadamente 10 minutos en crear un bloque, como Bitcoin (Anh Dinh *et al.*, 2018).

Adicionalmente los participantes en el mercado de segunda mano necesitarían un nodo minero para generar bloques y que se haga efectiva la transacción, por lo que podría funcionar solo con productos de segunda mano que compren las empresas, como maquinarias o productos de lujo. Para que el público pueda acceder a los beneficios indicados de la Blockchain se deben utilizar equipos con IoT (como *smartphones*, tabletas, sensores, etcétera) de fácil empleo para el público en general, los que poseen capacidad de comunicación para enviar la información al nodo minero más cercano, en donde se creará el bloque, como propone AgriBlockIoT

(Pincheira Caro *et al.*, 2018). Las personas que deseen solo leer la información almacenada en la Blockchain lo podrían hacer mediante dispositivos IoT conectados con claves pública y privada, para mayor seguridad, al nodo minero más cercano (Qu, Tao, Zhang, Hong y Yuan, 2018). En conclusión, la tecnología de Blockchain promete una mejor trazabilidad en la cadena de suministro, pero aún se encuentra en su estado inicial. En futuros trabajos podremos analizar la seguridad de esta plataforma en términos de confidencialidad y no solo de integridad, como señalamos, especialmente al conectar equipos de IoT con la tecnología referida, así como el manejo del gobierno de los datos, de acuerdo a la industria y el modelo de negocio.

REFERENCIAS

- Anh Dinh, T., Liu, R., Zhang, M., Chen, G., Chin Ooi, B., y Wang, J. (Julio de 2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering* 30(7), pp. 1366-1385. doi:10.1109/TKDE.2017.2781227
- Christidis, K., y Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access* 4, pp. 2292-2303. doi:10.1109/ACCESS.2016.2566339
- Engelenburg, S., Janssen, M., y Klievink, B. (2017). Design of a software architecture supporting business-to-government information sharing to improve public safety and security. *Journal of Intelligent Information Systems*. doi:10.1007/s10844-017-0478-z
- Firica, O. (Octubre de 2017). Blockchain technology: Promises and realities of the year 2017. *Quality-Access to Success* 18(S3), pp. 51-58.
- Goldman Sachs Group (2016). *Blockchain: Putting Theory into Practice*. Equity Research.
- Madhwal, Y., y Panfilov, P. B. (2017). Blockchain and supply chain management: Aircrafts' parts' business case. *28th DAAAM International Symposium on intelligent manufacturing and automation*. Viena. doi: 10.2507/28th.daaam.proceedings.146
- Morgan, J. P., y Wyman, O. (2016). *Unlocking Economic Advantage with Blockchain: A guide for asset managers*.
- Pincheira Caro, M., Salek Ali, M., Vecchio, M., y Giaffreda, R. (2018). Blockchain-based Traceability in Agri-Food Supply Chain Management: A Practical Implementation. *2018 IoT Vertical and Topical Summit on Agriculture*. Tuscany: IEEE.
- Qu, C., Tao, M., Zhang, J., Hong, X., y Yuan, R. (Junio de 2018). Blockchain Based Credibility Verification Method for IoT Entities. *Security and Communication Networks 2018*, pp. 1-11. doi: doi.org/10.1155/2018/7817614

- Shanley, A. (2017). Could Blockchain improve pharmaceutical supply chain security? *Pharmaceutical Technology*, pp. 34-39.
- Toyoda, K., Sasase, I., Ohtsuki, T., y Mathiopoulos, P. (2017). A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain. *IEEE Access* 5, pp. 17465-17477. doi:10.1109/ACCESS.2017.2720760
- Wu, H., Li, Z., King, B., Miled, Z. B., Wassick, J., y Tazelaar, J. (2017). A Distributed ledger for supply chain physical distribution visibility. *Information* 8(137), pp. 1-18. doi:10.3390/info8040137
- Yeow, A. (2018). Bitnodes. Recuperado de *earn.com*: <https://bitnodes.earn.com/>
- Yeow, K., Gani, A., Rodrigues, J., Ahmad, R., y Ko, K. (2017). Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues. *IEEE Access*, 6, 1513-1524. doi: 10.1109/Access.2017.2779263

BIBLIOGRAFÍA

- Anh Dinh, T., Wang, J., Chen, G., Liu, R., Chin Ooi, B., y Tan, K.-L. (2017). *Blockbench: A Framework for Analyzing Private Blockchains*. Chicago: ACM. doi:10.1145/3035918.3064033
- Beninger, P. (2017). Opportunities for Collaboration at the Interface of Pharmacovigilance and Manufacturing. *Clinical Therapeutics* 39(4), pp. 702-712. Recuperado de <http://dx.doi.org/10.1016/j.clinthera.2017.03.010>
- Kiyomoto, S., Rahman, M., y Basu, A. (2017). On Blockchain-based Anonymized Dataset Distribution Platform. *IEEE/ACIS 15th International Conference on Software Engineering Research, Management and Application (SERA)*, Londres.
- Kshetri, N. (2017). Can Blockchain Strengthen the Internet of Things? *IT Professional*, pp. 68-72.
- Zhang, J., Xue, N., y Huang, X. (2016). A secure system for pervasive social network-based healthcare. *IEEE Access* 4, 9239-9250. doi:10.1109/ACCESS.2016.2645904