Prueba de concepto para la trazabilidad de cadenas de suministro con tecnología *blockchain*

Proof of Concept for Supply Chain Traceability with Blockchain Technology

Cáceres Hernández, Arturo; Delgado Fernández, Tatiana; Lopes Martínez, Igor

Arturo Cáceres Hernández
arturoch294@gmail.com
UNIVERSIDAD TECNOLÓGICA DE LA HABANA "JOSÉ ANTONIO ECHEVERRÍA, Cuba

Tatiana Delgado Fernández
tatiana.delgado@uic.cu
UNIVERSIDAD TECNOLÓGICA DE LA HABANA "JOSÉ ANTONIO ECHEVERRÍA, Cuba

Igor Lopes Martínez
igorlm16@yahoo.es
UNIVERSIDAD TECNOLÓGICA DE LA HABANA "JOSÉ ANTONIO ECHEVERRÍA", Cuba

Revista Cubana de Transformación Digital
Unión de Informáticos de Cuba, Cuba
ISSN-e: 2708-3411
Periodicidad: Trimestral
vol. 3, núm. 3, 2022
rctd@uic.cu

Recepción: 03 Diciembre 2021
Aprobación: 15 Agosto 2022

URL: http://portal.amelica.org/ameli/journal/389/3893627008/

Resumen: Una cadena de bloques autorizada es una red compartida inmutable, altamente se- gura y confiable, que proporciona a cada participante visibilidad de extremo a extremo según su nivel de permiso. Este artículo tiene como objetivo analizar una solución para las cadenas de suministros de los insumos de la agricultura cubana, en un caso de estudio, aplicando la tecnología *blockchain*. Tras describir los principales conceptos de la tecnología *blockchain* se analizan sus ventajas fundamentales, como la integridad, la seguridad y la descentralización, para ser aplicada en cadenas de suministros. Con vistas a entender las necesidades del flujo de trazabilidad de los productos en el sector agrícola, fueron aplicadas entrevistas dirigidas a una empresa de logística del tabaco en Cuba. Como una aproximación para resolver el problema detectado respecto a la trazabilidad y la necesidad de incrementar la confianza en la integridad del producto, a lo largo de la cadena, se desarrolla una prueba de concep- to sobre la plataforma pública Ethereum, aplicada al modelo de cadena de suminis- tros de una empresa de servicios técnicos y logística especializada del tabaco.

Palabras clave: *blockchain*, cadena de suministro, contrato inteligente, prueba de concepto.

Abstract: *A blockchain is an immutable, highly secure and reliable shared network that provides each participant with end-to-end visibility based on their permission level. This article aims to analyze a solution for the supply chains of agricultu- ral inputs in a case study in Cuba, applying blockchain technology. After des- cribing the main concepts of blockchain technology, its fundamental advanta- ges are analyzed, such as integrity, security and decentralization, to be applied in supply chains. With a view to raising the problem of the traceability flow of products in the agricultural sector, interviews were conducted with a tobacco logistics company in Cuba. As an approach to solve the problems detected re- garding traceability and the need to increase confidence in the integrity of the product throughout the chain, a proof of concept is developed on the public Ethereum platform applied to the supply chain model of a specialized tobacco logistics and technical services company.*

Keywords: blockchain, supply chain, smart contract, proof of concept.

INTRODUCCIÓN

La cadena de suministro vincula las fuentes de suministro (proveedores) con los propietarios de la demanda (clientes finales). El objetivo de cualquier cadena de suministro es entregar los suministros correctos, en las cantidades correctas, a los lugares correctos, en el momento co- rrecto. Las cadenas de suministro comprenden todas las actividades y los procesos asociados con el flujo y la transformación de bienes desde la etapa de materia prima hasta el usuario final (Balcik & Beamon, 2008)

La cadena de suministro está relacionada con todos los procesos de negocio de las organi- zaciones. Los recursos humanos, la tecnología, la estructura comercial y los recursos, son un todo inseparable con el concepto de cadena de suministro en esta estructura que comienza desde el proveedor hasta el cliente. La gestión de la cadena de suministro es la optimización de todos los procesos en los procesos de un producto o servicio, desde el fabricante hasta el consumidor. Esta optimización significa aumentar la satisfacción de clientes y proveedores mientras se minimizan los costos. La gestión de la cadena de suministro es muy importante, ya que mejora el servicio al cliente, reduce los costos de inventario y la planificación y los gas- tos operativos, acorta los procesos de toma de decisiones y aumenta la competitividad como resultado de todo esto (Ayyildiz, E., & Taskin Gumus, A., 2021).

A medida que las empresas actuales se han hecho dependientes de una gran variedad de

bienes y servicios para complementar sus actividades de agregación de valor, la mayoría ha

desarrollado grandes redes de suministradores y clientes, que son creaciones frágiles sujetas a peligros de interrupción debido a muchas razones. Las empresas funcionan como parte de un sistema integral y, por tanto, son vulnerables a interrupciones por causas externas, que afec- tan a toda la cadena (Gereffi, 2001).

Una solución efectiva y versátil a los problemas más frecuentes de cadenas de suminis- tro puede ser *blockchain*. Una cadena de bloques o *blockchain* "[...] es un libro mayor digital, distribuido, que registra transacciones en una red *peer-to-peer* pública o privada. Este libro mayor registra permanentemente los registros/historial de transacciones entre dos nodos, en

una cadena secuencial de bloques enlazados mediante hashes criptográficos y se distribuye a todos los nodos de la red. Todas las transacciones confirmadas y validadas son enlazadas en- tre sí y colocadas en la cadena. La cadena de bloques actúa como una única fuente de verdad, y los miembros de la red solo pueden ver aquellas transacciones que son relevantes para ellos" (Brakeville & Perepa, 2016).

Aunque surgió como tecnología para sistemas de dinero electrónico basados en criptomo- nedas, cada vez más su uso se está diseminando en diferentes áreas de negocio, erigiéndose como una de las tecnologías habilitadoras más importantes en la era de la transformación di- gital. Su potencial para brindar confianza en ambientes donde los participantes no necesaria- mente confían entre sí, ha llevado a empresas, organizaciones, y más recientemente a gobier- nos, al uso de esta tecnología para resolver problemas existentes, que a su vez ha propiciado el surgimiento de herramientas que asisten el desarrollo de aplicaciones y plataformas basadas en *blockchain* (Monleón-Durá, 2020). *Blockchain* está considerada como una de las tecnolo- gías habilitadoras de la transformación digital (Delgado-Fernández, 2020).

En el ámbito de las cadenas de suministro de la agricultura, *blockchain* está siendo apli-

cado de forma cada vez más significativa. La compañía danesa Maersk, el transportista de contenedores más grande del mundo que representa del 18 % al 20 % del mercado, es un ejemplo destacado de una empresa que prueba con éxito aplicaciones *blockchain* en logís- tica internacional para las posiciones GPS, temperaturas y otros datos de los contenedores. Maersk también ha estado buscando una mejor solución para rastrear la velocidad de las operaciones de carga y descarga. como el seguimiento de barcos y, por tanto, de contene- dores transportados. IBM y Maersk, en septiembre de 2016, realizaron una prueba de con- cepto siguiendo un contenedor cargado de flores desde Puerto de Mombasa, en Kenia, a Rotterdam, en Holanda. El costo de envío en esa prueba fue de 2 000.00 USD y el costo de la documentación se calculó en aproximadamente 300.00 USD (Groenfeldt, 2017). La solu- ción desarrollada por Maersk e IBM se basa en Hyperledger Fabric

de código abierto, de la Fundación Linux. El anuncio de IBM decía que la solución está diseñada para ayudar a re- ducir o eliminar el fraude y los errores, minimizar el tiempo que los productos pasan en el proceso de tránsito y envío, mejorar la gestión de inventario y, en última instancia, reducir el desperdicio y los costos (Groenfeldt, 2017).

Con sus capacidades de descentralización, intercambio de datos y prevención de ma- nipulación de datos, la cadena de bloques se puede aplicar para eliminar la asimetría de

la información en la mayor medida posible y mejorar la sostenibilidad de la cadena de su- ministro. En la actualidad, las comunidades académicas han contribuido a una gran can- tidad de investigaciones sobre la aplicación de la tecnología *blockchain* en la innovación de la gestión de la cadena de suministro (Song, Luo, Chang, Jin, & Nicolas, 2022).

Siendo una tecnología compleja, particularmente para ser adoptada por empresas habitua- das a otros entornos tecnológicos, y a partir del análisis de las potenciales ventajas que traería su despliegue en cadenas de suministro, el objetivo de este artículo es experimentar, a través de una prueba de concepto, su potencial uso para la trazabilidad de productos, en este caso, en un escenario de cadena de suministros del sector tabacalero en Cuba.

Esta prueba de concepto tiene su principal valor práctico en la medida en que demuestra que *blockchain* es una tecnología capaz de transformar los procesos empresariales y, en par- ticular, aquellos relacionados con las cadenas de suministro, permitiendo una trazabilidad de extremo a extremo, soportada en una cadena de bloques autorizada como red compartida in- mutable, altamente segura y confiable.

METODOLOGÍA

Definición de blockchain

Una cadena de bloques o *blockchain* es: "[...] un sistema en el cual un registro de tran- sacciones de bitcoins u otras criptomonedas es mantenido en varias computadoras en- lazadas entre sí en una red *peer-to-peer*" (Nakamoto, 2008). Esta definición incorpora el concepto de red P2P, pero no aplica totalmente a este proyecto, debido a que se enfoca únicamente en transacciones de criptomonedas. Una *blockchain* es: "[...] esencialmente una base de datos distribuida de registros o libro mayor de transacciones o eventos que hayan sido ejecutados y compartidos entre participantes. Cada transacción en el libro mayor es verificada por consenso de la mayoría de los participantes en el sistema. Una vez que la información es ingresada en el sistema, no puede ser nunca eliminada". En esta definición se incorporan conceptos clave, como "base de datos distribuida" o "li- bro mayor", además de la idea de información que no puede ser eliminada, así como el concepto de verificar transacciones por consenso. Sin embargo, cuando se menciona el concepto de consenso, se restringe al caso de consenso de la mayoría de participantes en el sistema, lo cual aplica generalmente en *blockchain* públicas, pero no siempre en privadas, clasificación sobre la cual se profundiza en este artículo (Crosby, Pattanayak, Verma, & Kalyanaraman, 2016).

Existen determinadas características que hacen de las cadenas de bloques una tecnología prometedora capaz de proporcionar nuevas soluciones a ciertos problemas, como las transfe- rencias de información internacional sin una autoridad central que haga de intermediario o la auditabilidad de las cadenas de suministros, garantizando su inmutabilidad, por citar algunos de los ejemplos más conocidos. De las características que son posibles identificar en "Bitcoin: a peer to peer cash system" (Nakamoto, 2008) se destacan las siguientes:

- • Descentralización: las transacciones en una red de *blockchain* pueden efectuarse entre pares de esta, sin necesidad de contar con la intervención de una autoridad central.

• Inmutabilidad: las transacciones que se intercambian a través de la red atraviesan un pro- ceso de validación, confirmación y almacenamiento, distribuido en diferentes nodos de la red, de tal modo que resulta casi imposible modificar las transacciones almacenadas.

• Auditabilidad: consultando las transacciones almacenadas en la *blockchain*, participantes de la red y usuarios de aplicaciones que interactúan con la *blockchain*, pueden verifi- car y llevar una trazabilidad de registros almacenados.

• Procedencia: provee de una forma de trazar el origen de cada transacción.

• Base de datos distribuida: cada nodo participante tiene acceso a una base de datos dis- tribuida, que ningún par individual controla y cualquiera de ellos puede verificarla o re- generarla en caso de ser necesario, sin ningún intermediario central, en tiempo real.

Una red P2P (*peer-to-peer*) es un método para compartir archivos a través de Internet, constituyendo un tipo específico de una red descentralizada. En este tipo de redes no existe un servidor central, y cada nodo de la red utiliza *software* especializado para conectarse con el resto de los nodos (Steinmetz & Wehrle, 2005). La figura 1 muestra la arquitectura de una red basada en P2P y la de una red basada en un servidor central.

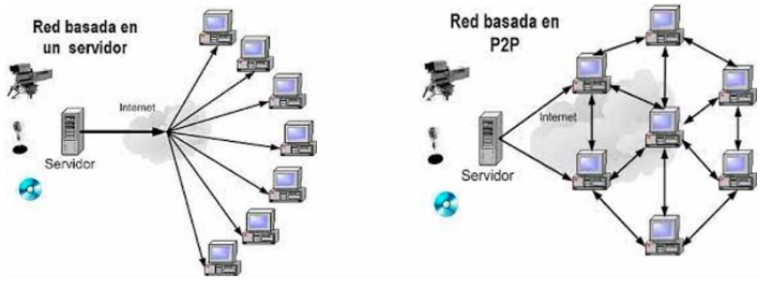

Figura 1. Comparación de red P2P y red basada en un servidor central.

FIGURA 1.
Comparación de red P2P y red basada en un servidor central.
sf

Mecanismos de consenso

El consenso es el proceso, mediante el cual una red de nodos garantiza el orden correcto de las transacciones y valida los bloques que las contienen (Cachin, & Vukolić, 2017). Siempre que exista una propuesta de actualización de la cadena es necesario llegar a un acuerdo respecto a la legitimidad de esa actualización entre nodos de la red, utilizando para ello un mecanismo 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 (Dinh, Liu, Zhang, Chen, Ooi, & Wang, 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 ver- sión original de *blockchain* desarrolla el protocolo PoW, basado en los cálculos computa- cionales del CPU; luego pasó a la tarjeta de video del computador y hoy al procesador ASIC (*Application-Specific Integrated Circuit*). Otro de los protocolos más comunes es el *Practical Byzantine Fault Tolerance* (PBFT), que se maneja con las *blockchain* privadas y está basado principalmente en comunicación. En una red privada no es necesario usar recompensas, por- que 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).

Contratos inteligentes

Los Contratos Inteligentes se pueden definir como un programa informático que facilita, ase- gura, hace cumplir y ejecuta acuerdos registrados entre dos o más partes, por ejemplo, de esto sería un acuerdo entre personas u organizaciones encargadas de exportación e importación de productos. Como tal, los Contratos Inteligentes ayudarían en la negociación y definición de tales acuerdos, que causarán que ciertas acciones sucedan como resultado de que se cumplan o incumplan una serie de condiciones específicas y previamente pactadas. Los contratos elec- trónicos están vinculados a las páginas web y luego a las aplicaciones y respectivas platafor- mas. La transcendental novedad referente a la desmaterialización del contrato versa sobre la presentación electrónica de los términos y las condiciones, los cuales en este tipo de contratos son expresados en lenguaje alfanumérico y establecidos en una cadena de bloques inmodifi- cable. En cambio, la forma de los contratos inteligentes se determina por la manera como se concrete la arquitectura o forma de la cadena de bloques o *blockchain*; en estos, igualmente, se continúa con la desmaterialización de la forma del contrato tradicional, pero en este caso para su presentación se utiliza ya no un lenguaje alfanumérico como en los anteriores, sino un lenguaje matemático y de programación, los cuales podrían llegar a ser más complejos y en especial para los abogados (Ramírez, 2019).

Transacciones en*blockchain*

Una moneda electrónica es una cadena de firmas digitales. Cada propietario transfiere la mo- neda al siguiente propietario, firmando digitalmente un *hash* de la transacción previa y la clave pública del siguiente propietario, y añadiendo ambos al final de la moneda. El beneficiario pue-

de comprobar las firmas para verificar la cadena de propiedad. El problema, por supuesto, es que el beneficiario no puede verificar que uno de los propietarios no haya gastado dos veces la misma moneda. La solución habitual es introducir una autoridad central de confianza, o casa de la moneda, que comprueba cada transacción para que eso no se produzca. Tras cada tran- sacción, la moneda debe regresar a la casa de la moneda para distribuir una nueva moneda y solo las monedas emitidas directamente desde ella están libres de la sospecha de doble gasto. El problema de esta solución es que el destino de todo el sistema de dinero depende de la com- pañía que gestiona la casa de la moneda, por la cual pasa cada transacción, igual que un banco. Se requiere una forma en que el beneficiario sepa que los propietarios previos no han fir- mado transacciones anteriores. Para nuestros propósitos, la transacción más temprana es la que cuenta, así que no nos preocupamos de los intentos de doble gasto posteriores. La única manera de confirmar la ausencia de una transacción es tener conocimiento de todas las tran- sacciones. En el modelo de la casa de la moneda, esta tiene conocimiento de todas las tran- sacciones y decide cuáles llegaron primero. Para lograrlo, sin la participación de una parte de confianza, las transacciones han de ser anunciadas públicamente, y necesitamos un sistema para que los participantes estén de acuerdo en un único historial del orden en que fueron re- cibidas. El beneficiario necesita prueba de que en el momento de la transacción la mayor parte de los nodos estaban de acuerdo en que esa fue la primera que se recibió (Nakamoto, 2008).

En la figura 2 se ilustran las transacciones en blockchain.

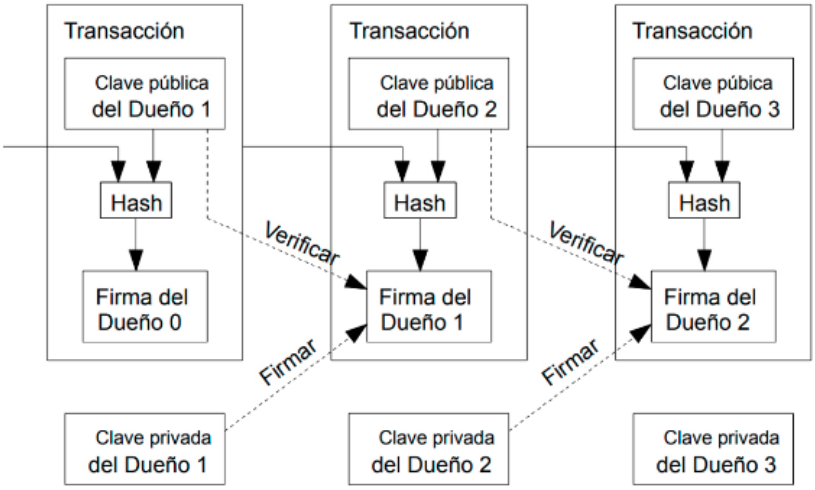

Figura 2. Transacciones en blockchain (adaptado de Nakamoto, 2008).

FIGURA 2.
Transacciones en blockchain (adaptado de Nakamoto, 2008).
sf

La solución que proponemos comienza con un servidor de sellado de tiempo, que trabaja tomando el *hash* de un bloque de ítems para sellarlos en el tiempo y notificar públicamente

su *hash*, como un periódico o un *post* Usenet. El sellado de tiempo prueba que los datos han existido en el tiempo, obviamente, para entrar en el *hash*. Cada sellado de tiempo incluye el sellado de tiempo previo en su *hash*, formando una cadena con cada sellado de tiempo adicio- nal, reforzando al que estaba antes (Nakamoto, 2008).

Funciones *hash*

Las funciones de *hash* criptográficas siguen siendo una de las primitivas criptográficas más im- portantes, que se pueden utilizar para garantizar la seguridad de muchas aplicaciones y proto- colos criptográficos, como la firma digital, la generación de números aleatorios, la autenticación de fuentes de datos, la actualización y derivación de claves, el código de autenticación de mensa- jes, la protección de integridad, el reconocimiento de código malicioso, SSL, TLS y S/MIME. Las funciones *hash* criptográficas comprimen un mensaje de entrada de longitud arbitraria en una salida con una longitud fija corta, el código *hash*. Las funciones *hash* se clasifican en dos clases: función hash sin clave, también conocida como Código de Detección de Manipulación (MDC) con un solo parámetro: un mensaje y una función *keyedhash* con dos entradas distintas: un mensaje y una clave secreta. Las funciones *hash* con clave se utilizan para construir el Código de Autenticación de Mensajes (MAC), que se utiliza ampliamente para proporcionar integridad de datos y autenticación de origen de datos. La elección entre un MAC y un MDC depende de la aplicación. También se clasifican como funciones *hash* basadas en cifrado de bloques, funcio- nes *hash* basadas en algoritmos modulares y funciones *hash* dedicadas. La motivación detrás de los esquemas basados en cifrado de bloques es la minimización del esfuerzo para diseñar e implementar las funciones *hash* y de la complejidad del equipo. Además, la confianza que uno tiene en un determinado cifrado de bloque (como DES) se puede transferir a una función hash. Particularmente interesantes desde un punto de vista teórico, los esquemas basados en algo- ritmos modulares son demostrablemente seguros, en el sentido de que su seguridad se basa en la dureza de algunos problemas matemáticos, como los problemas de teoría de números. Las funciones *hash* dedicadas están especialmente diseñadas desde cero, con el propósito de hacer hash de un texto sin formato con un rendimiento optimizado y sin estar restringidas a reutili- zar componentes del sistema existentes, como cifrados en bloque y aritmética modular (Tiwari & Asawa, 2012).

DApp

El acrónimo DApp se deriva del inglés de aplicaciones descentralizadas. Las DApp se refieren a aplicaciones que se ejecutan en la red *peer-to-peer* (P2P) de computadoras, en lugar de una sola computadora centralizada. Muchos se han desarrollado y difundido ampliamente DApp famosas, como Bit Torrent para compartir archivos, Bit Message para mensajería instantánea y Popcorn Time para transmisión de video.

Blockchain proporciona una abstracción de cálculo general a través del mecanismo de los con-

tratos inteligentes, lo que facilita el desarrollo DApp para varios contextos de aplicación. Por ejem- plo, Ethereum proporciona contratos inteligentes a desarrolladores para implementar programas

de propósito general. En consecuencia, con el auge de *blockchain* han surgido más y más DApp basadas en esta tecnología, siendo adoptado en casi todas las áreas (Wu, Ma, Huang, & Liu, 2019).

Blockchain aplicado a cadenas de suministros

Dadas las características y funciones que pone *blockchain* al alcance de las manos hay diver- sas formas de uso para la logística, que van desde la aplicación interna en los eslabones de la cadena, a abarcar toda la información que se mueve en esta de forma descentralizada, con la posibilidad de añadir trazabilidad de la historia de un producto, su proceso de fabricación y la cadena logística, garantizando además la confianza entre todos los actores sin que exista una entidad central que controle el proceso (Hackius & Petersen, 2017).

Todos los implicados (proveedores, productores, operadores y minoristas) se encadenan para crear una huella digital que se actualiza y muestra la información en tiempo real dispo- nible para toda persona perteneciente a la cadena en su camino al consumidor final.

Una plataforma *blockchain* que involucre a todos los actores de la cadena puede además

trabajar en conjunto con elementos de IoT y usar la tecnología de Smart Contracts para pre- fijar acuerdos entre las diferentes partes, garantizando que esos acuerdos son satisfechos o para controlar las regulaciones. La automatización de transacciones de mercancías, pedidos o pagos, o el control del cumplimiento de la cadena de frío o las regulaciones ambientales son solo algunos ejemplos.

Un modelo como el descrito presenta capacidad para mejorar la eficiencia y reducir los costos en distintos ámbitos de operación. La utilización del registro inmutable y confiable de *blockchain* permite garantizar quién es el responsable en cada momento del bien transporta- do. Por otro lado, una mayor integración entre los participantes a nivel de stocks e inventario puede mejorar los procesos desde una visión más amplia, sincronizando y automatizando la relación entre flujos de inventario, flujos financieros y datos, para conseguir una optimización a nivel de costos y una mejor evaluación de riesgos. La tabla1 muestra resumidamente las principales ventajas y desventajas de la tecnología *blockchain*.

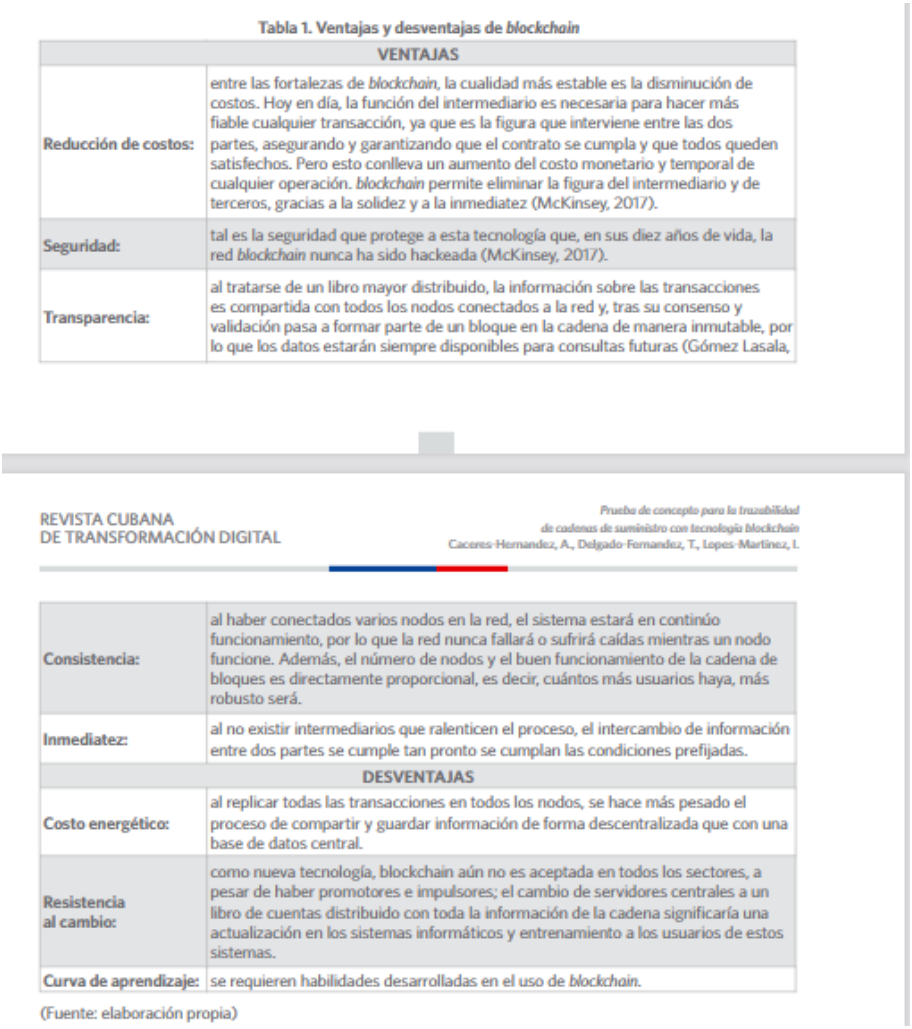

Tabla 1. Ventajas y desventajas de *blockchain*

VENTAJAS	
Reducción de costos:	entre las fortalezas de *blockchain*, la cualidad más estable es la disminución de costos. Hoy en día, la función del intermediario es necesaria para hacer más fiable cualquier transacción, ya que es la figura que interviene entre las dos partes, asegurando y garantizando que el contrato se cumpla y que todos queden satisfechos. Pero esto conlleva un aumento del costo monetario y temporal de cualquier operación. *blockchain* permite eliminar la figura del intermediario y de terceros, gracias a la solidez y a la inmediatez (McKinsey, 2017).
Seguridad:	tal es la seguridad que protege a esta tecnología que, en sus diez años de vida, la red *blockchain* nunca ha sido hackeada (McKinsey, 2017).
Transparencia:	al tratarse de un libro mayor distribuido, la información sobre las transacciones es compartida con todos los nodos conectados a la red y, tras su consenso y validación pasa a formar parte de un bloque en la cadena de manera inmutable, por lo que los datos estarán siempre disponibles para consultas futuras (Gómez Lasala,

Consistencia:	al haber conectados varios nodos en la red, el sistema estará en continúo funcionamiento, por lo que la red nunca fallará o sufrirá caídas mientras un nodo funcione. Además, el número de nodos y el buen funcionamiento de la cadena de bloques es directamente proporcional, es decir, cuántos más usuarios haya, más robusto será.
Inmediatez:	al no existir intermediarios que ralenticen el proceso, el intercambio de información entre dos partes se cumple tan pronto se cumplan las condiciones prefijadas.
DESVENTAJAS	
Costo energético:	al replicar todas las transacciones en todos los nodos, se hace más pesado el proceso de compartir y guardar información de forma descentralizada que con una base de datos central.
Resistencia al cambio:	como nueva tecnología, blockchain aún no es aceptada en todos los sectores, a pesar de haber promotores e impulsores; el cambio de servidores centrales a un libro de cuentas distribuido con toda la información de la cadena significaría una actualización en los sistemas informáticos y entrenamiento a los usuarios de estos sistemas.
Curva de aprendizaje:	se requieren habilidades desarrolladas en el uso de *blockchain*.

(Fuente: elaboración propia)

TABLA 1.
Ventajas y desventajas de blockchain
elaboración propia

A pesar del progreso que significaría la adopción de la tecnología *blockchain* en muchos ám- bitos de la vida económica, incluyendo las cadenas de suministro, siguen habiendo elementos que se oponen a esta transformación. El principal reto que se debe enfrentar es cambiar la mentalidad de los participantes, ya que para su correcto funcionamiento, todos los eslabones de la cadena de suministro deberían actualizar sus sistemas de registro y tratamiento de la información.

A pesar del progreso que significaría la adopción de la tecnología blockchain en muchos ám- bitos de la vida económica, incluyendo las cadenas de suministro, siguen habiendo elementos que se oponen a esta transformación. El principal reto que se debe enfrentar es cambiar la mentalidad de los participantes, ya que para su correcto funcionamiento, todos los eslabones de la cadena de suministro deberían actualizar sus sistemas de registro y tratamiento de la información.

Guía metodológica de la prueba de concepto de blockchain en el caso de estudio

Para la experimentación de blockchain en la cadena de suministros de una empresa tabacale- ra cubana, se siguen los pasos que aparecen en la figura 3.

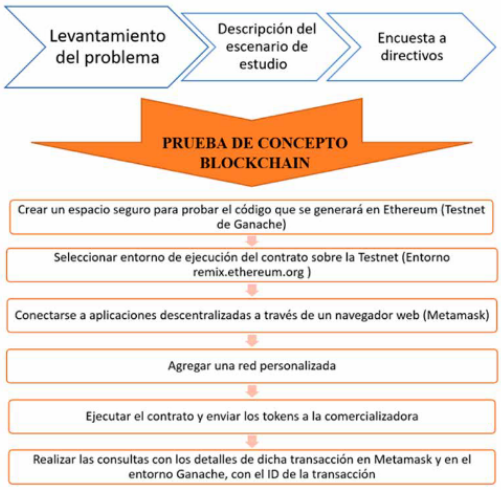

Figura 3. Metodología de la prueba de concepto de blockchain en el escenario de estudio.

FIGURA 3.
Metodología de la prueba de concepto de blockchain en el escenario de estudio.
sf

Levantamiento del problema asociado a la cadena de suministros del caso de estudio

Se realizaron entrevistas a directivos de la UEB Comercial Agrícola, de la empresa de servi- cios técnicos y logística especializada del tabaco, siguiendo el guión siguiente:

- • ¿Cómo funcionan las cadenas de suministro de la agricultura en Cuba?
  - • ¿Qué necesidad de información afecta a esta empresa?
  - • ¿Cómo se llevan los registros de inventario?
  - • ¿Se rastrea el producto recibido?
  - • ¿Los códigos para gestionar el inventario de productos se mantienen desde el proveedor hasta el consumidor final?

A partir de la información obtenida en las encuestas se pudo generalizar la cadena de su- ministros de insumos para la agricultura (figura 4).

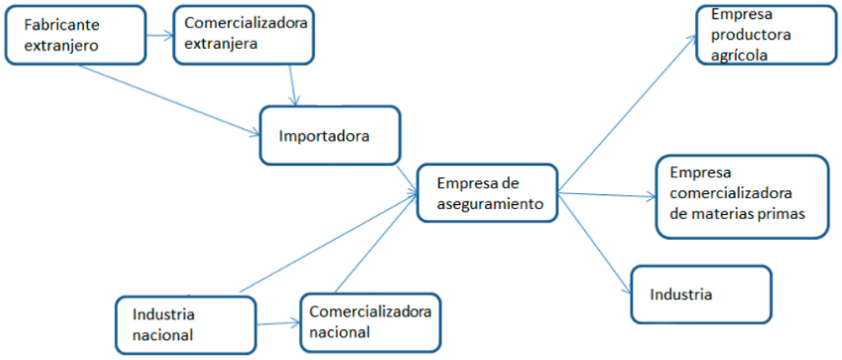

Figura 4. Representación de cadena de suministros de insumos para la agricultura.

FIGURA 4
Representación de cadena de suministros de insumos para la agricultura.
sf

Para la compra de los insumos de la agricultura se utiliza una empresa intermediaria que contacta la importadora y hace pedidos en base a la demanda de sus clientes, o contacta a la comercializadora o industria nacional en caso de que el insumo se fabrique en el país, para luego distribuir. El objetivo de esto es que se reduzcan los costos por pedidos por cantidades.

Se pudieron identificar los siguientes problemas:

- • No existe estandarización en la cadena de suministros: las identificaciones de los pro- ductos cambian en cada paso de la cadena, cada organismo tiene un método para gestio- nar sus almacenes y etiquetar los insumos que se comercian.
  • Falta de trazabilidad: al no haber estandarización, no hay forma de trazar o rastrear el producto.
  • Falta de información con respecto al estado o localización del insumo: además de no poder describir el recorrido, ninguna de las partes que no controle el insumo en el mo- mento, puede saber dónde se encuentra.
  • Falta de información en tiempo real de la demanda del cliente final: se contrata con los proveedores en base a una información de demanda que no se actualiza en tiempo real y deja poco espacio a ajustes necesarios.

PLanteamiento de La soLución

Una aplicación de *blockchain* a este caso podría optimizar los procesos que ocurren en esta cadena, por el hecho de eliminar intermediarios. Utilizando los equipos de cómputo que ya existen en los clientes finales se crearía una red *peer-to-peer*, donde se comparta la informa- ción en tiempo real y se guarde en cada uno de esos equipos. Un mecanismo de consenso como minería de datos, para tomar datos de demanda en tiempo real, permitiría que se sepa la cantidad necesaria para comprar a la hora de realizar el contrato. Esta red utilizaría con- tratos inteligentes que permitan dar un grupo de condiciones que se deben cumplir antes de la contratación con el proveedor, fijar términos y realizar la operación sin intermediarios, ga- rantizando que se contrate todo lo necesario de una vez (pedidos por cantidad), agilizando el proceso y abaratando costos de comisiones de intermediarios.

La ejecución de cada acción en la red no permitiría solo saber qué paso del proceso se está ejecutando, sino también identificar los movimientos de los insumos como transacción en *blockchain*, identificando una cadena de firmas digitales con un *hash* asociado a cada tran- sacción y un identificador único a cada producto, garantizando estandarización, trazabilidad y rastreabilidad.

Para una trazabilidad de insumos en la cadena de suministro usando tecnología *block-*

chain se debe configurar una red P2P (peer-to-peer), donde cada parte de la cadena en la que es objetivo aplicar la tecnología instale su propio nodo, los requisitos pueden variar en depen- dencia de la complejidad del *software* que se va a instalar.

DesarroLLo de La prueba de concepto de uso de *blockchain* para trazabiLidad en cadenas de suministros

Para la prueba de concepto, cuyo objetivo es demostrar que el código creado con tecnología *blockchain* permite la trazabilidad en una cadena de suministros, se siguen los siguientes pasos:

1. Crear un espacio seguro para probar el código que se generará en Ethereum. En esta prueba de concepto se utiliza Testnet de Ganache, un *software* que proporciona una red de pruebas local sencilla e intuitiva. Testnet es un entorno que permite a los desarrolladores de aplicaciones descentralizadas (DApp) aumentar el valor de sus aplicaciones, probando que el código funciona. En la figura 5 se muestran las cuentas creadas en Ethereum con Ganache.

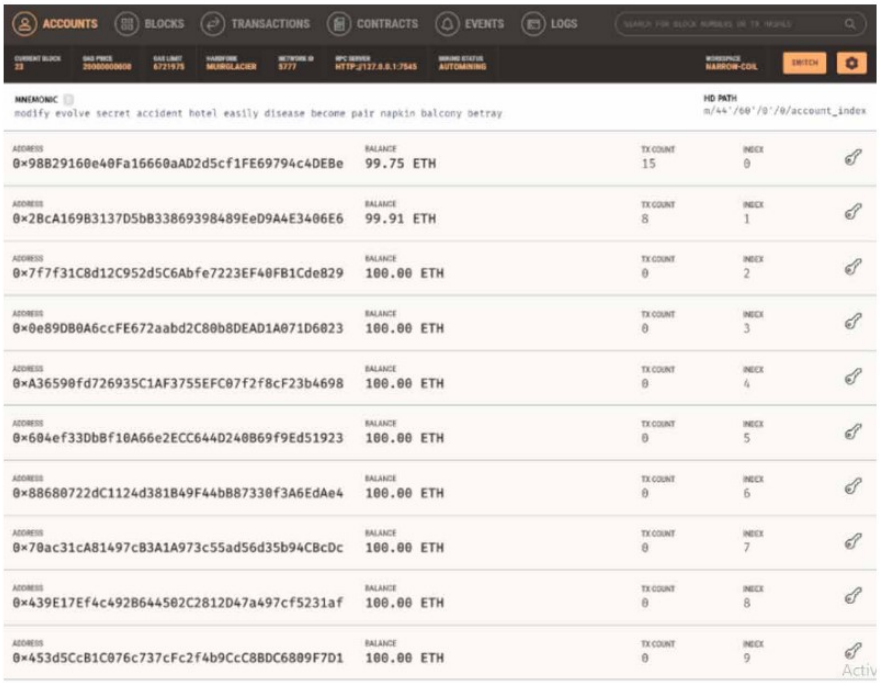

Figura 5. Muestra de entorno de prueba con Ganache.

FIGURA 5.
Muestra de entorno de prueba con Ganache.
sf

2. Usando remix.ethereum.org como entorno de desarrollo integrado se programa un con- trato para ejecutar sobre la testnet previamente creada. En esta prueba de concepto se toma un número de tokens como insumos para rastrear en la cadena, por lo tanto, el contrato que ejecutará será la minería de esos tokens en la dirección de los proveedores, donde se inicia el rastreo.

3. Habilitación de un servicio Metamask,1 que permite conectarse a aplicaciones descen- tralizadas a través de un navegador web. Este servicio permite gestionar varios aspectos de la prueba de concepto.

4. Agregar una red personalizada que se vincula a la tesnet de forma local, como se mues- tra en la figura 6.

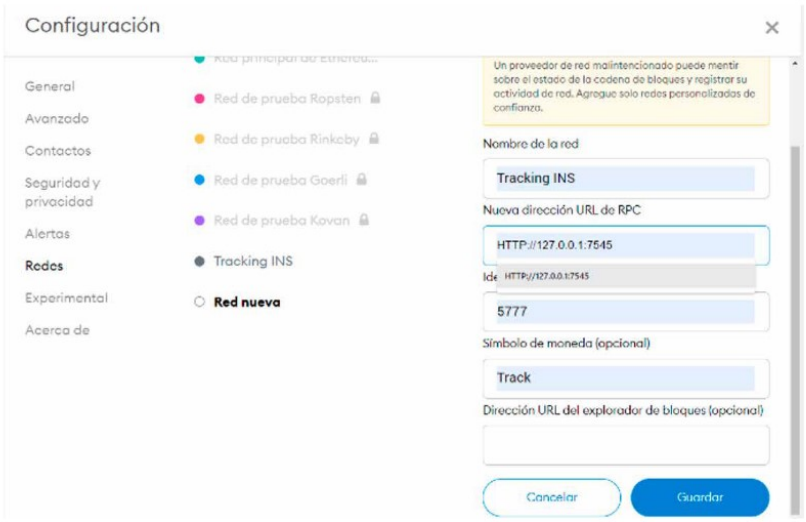

Figura 6. Vinculación de la tesnet a la red local.

FIGURA 6
Vinculación de la tesnet a la red local
sf

5. Introducir los datos de la *tesnet* que se obtienen de Ganache. Usando las llaves privadas de cada cuenta añadida al crear la tesnet, es posible añadir cada cuenta a Metamask y asignarle un nombre; en este caso se le ha asignado a cada una el nombre de un partici- pante en la cadena (figura 7).

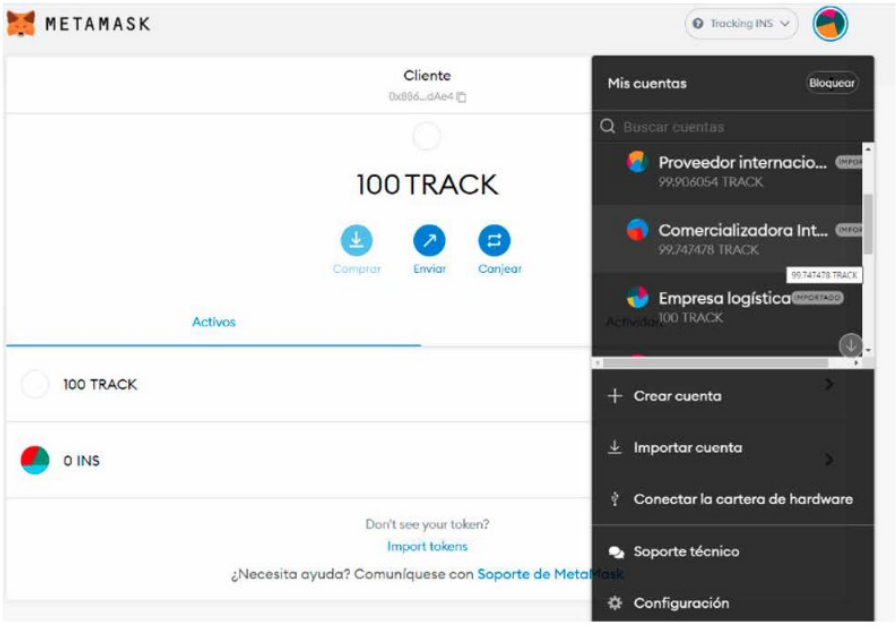

Figura 7. Personalización de las cuentas en el entorno Metamask.

FIGURA 7.
Personalización de las cuentas en el entorno Metamask.
sf

6. Ejecutar el contrato. En esta prueba de concepto se toma un número de *tokens* como in- sumos para rastrear en la cadena, por lo tanto, el contrato que ejecutará será la minería de esos *tokens* en la dirección de los proveedores, donde se inicia el rastreo, como apare- ce en la figura 8.

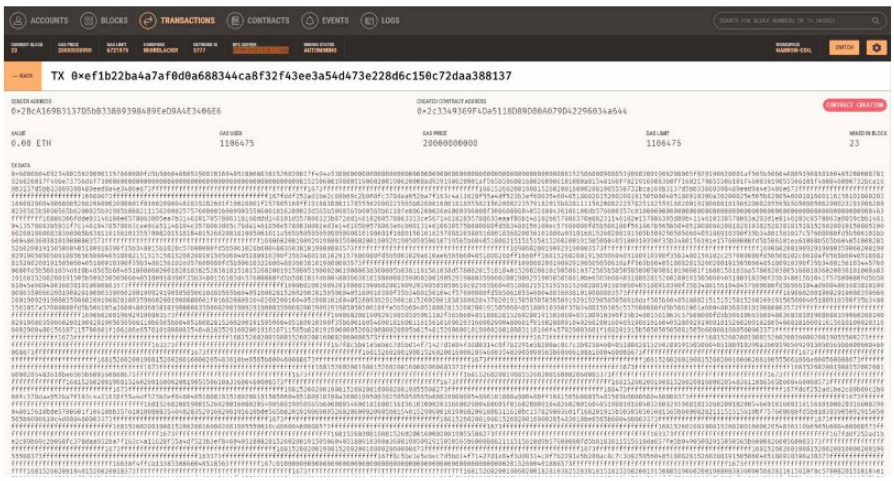

Figura 8. Ejecución del código del contrato.

FIGURA 8.
Ejecución del código del contrato.
sf

7. Cuando se ejecuta el contrato, este queda guardado en la *tesnet* y es visible para todos los participantes. Se decidió minar 50 *tokens* con nombre INS en la dirección del proveedor internacional (figura 9).

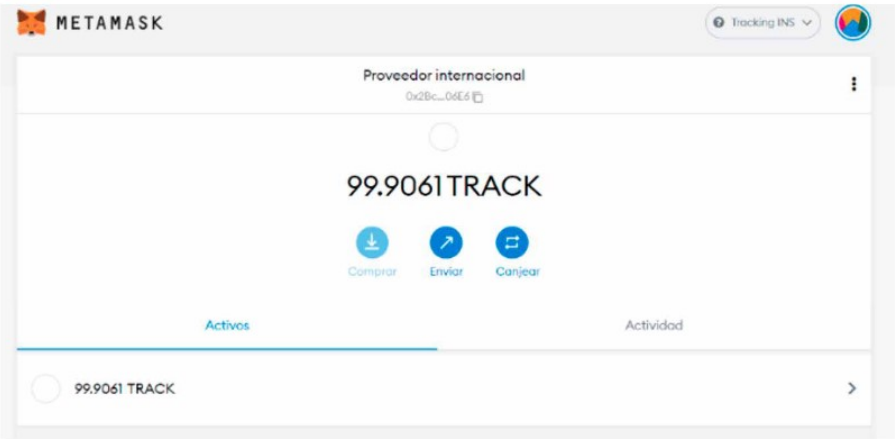

Figura 9. Minado de 50 *tokens* en la dirección del proveedor internacional.

FIGURA 9.
Minado de 50 tokens en la dirección del proveedor internacional.
sf

8. Enviar los *tokens* a la comercializadora, como aparece en la figura 10.

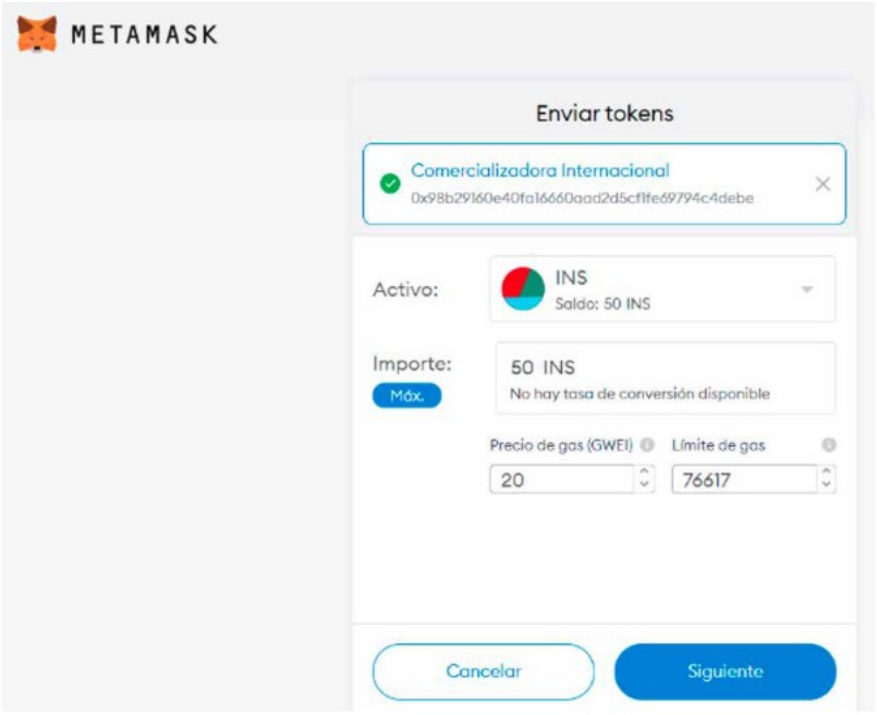

Figura 10. Envío de *tokens* a la comercializadora internacional.

FIGURA 10.
Envío de tokens a la comercializadora internacional.
Envío de tokens a la comercializadora internacional.

9. Realizar las consultas con los detalles de esa transacción en Metamask (figura 11) y en el entorno Ganache, con el ID de la transacción (figura 12).

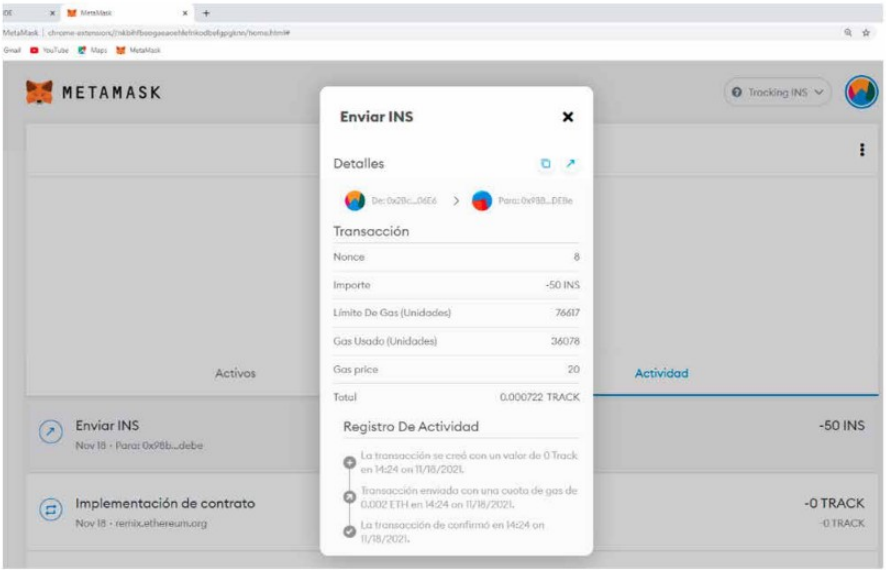

Figura 11. Consultas de la transacción en el entorno Metamask.

FIGURA 11.
Consultas de la transacción en el entorno Metamask.
sf

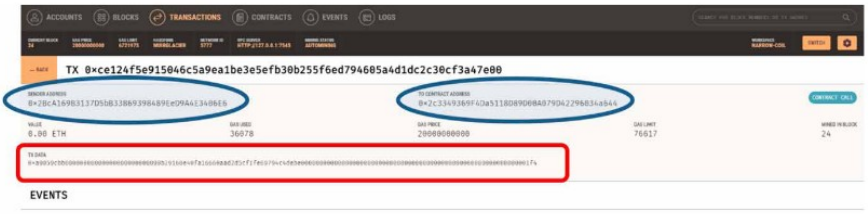

Figura 11. Consultas de la transacción en el entorno Metamask.

FIGURA 11.
Consultas de la transacción en el entorno Metamask.
sf

En la figura 12 se señala el origen y destino de la transacción en óvalos y la información encriptada del contrato inteligente, en un rectángulo. Cada contrato implementado o tran- sacción realizada puede ser rastreado de la misma forma, asegurando un seguimiento en la cadena y la disponibilidad de la información en tiempo real.

En la prueba de concepto se hizo una demostración de creación de un *token* y su respectiva

transferencia, dejando una trazabilidad inmortalizada en la *tesnet* de una *blockchain* de Ethe- reum. Al crear una *blockchain* de grado empresarial o usar una ya existente de base, varios parámetros son modificables, desde la función de cada nodo o los datos de trazabilidad que se usan.

Los *tokens* minados son creados en una dirección específica, a través de un contrato inte- ligente que ejecuta la acción de: Minar *tokens* en dirección predeterminada¨ y simplemente aparecen tokens en esa dirección, este contrato inteligente se puede programar para ser eje- cutable por un nodo con una función específica, por ejemplo: el nodo asignado al fabricante nacional o importadora mina un *token* en su dirección al producir un insumo X o importar un insumo X, respectivamente; este token se transfiere al transportarse, dejando un rastro inmutable en la blockchain empresarial (en todos los nodos a la vez). Solo estos nodos pueden minar un *token* en su dirección; este proceso se puede automatizar usando IoT.

Los contratos inteligentes no solo permiten minar *tokens* en una dirección específica, cual-

quier actividad puede ser automatizada, validada y asignada a cualquier nodo o pareja de no- dos que la efectúen, desde la minería de un *token* hasta su transferencia que se haya recibido o pagado. La programación de estos contratos se puede ejecutar con datos fuera de la cadena,

o sea, cada empresa puede mantener su *software* de gestión y tomar los valores que necesite para condicionar dichos contratos, por lo que no se afecta la manera en que cada empresa ges- tiona su información, solo es necesario la instalación de un nodo para participar en la cadena y se obtienen las ventajas mencionadas en esta investigación.

La versatilidad de esta tecnología permite también la instalación de un nodo para audito- ría en tiempo real, que tendría acceso solamente para observar cada transacción realizada y no a validarla o ejecutar acción alguna.

El problema específico al que se dirige esta investigación es la falta de trazabilidad en las cadenas de suministro nacionales. Las otras propuestas de solución a este problema se enfo- can en certificaciones y *software* de servidor central.

Una certificación de trazabilidad tiene la ventaja de demostrar la procedencia de un pro-

ducto amparado por una entidad de prestigio que lo emite. Una empresa puede emitir un certificado de trazabilidad sobre su propio producto en forma de sello. Las variantes de certi- ficación permiten conocer de dónde viene un producto, pero también son susceptibles a fal- sificación y deterioro, además de la gran desventaja que representa la falta de información en tiempo real y la pérdida de tiempo por mecanismos burocráticos.

Los *software* con servidor central son muy utilizados en la actualidad, tienen tantas ven-

tajas como una certificación, con la ventaja extra de la disponibilidad de información en tiempo real. Los *software* de trazabilidad con servidor central se suelen diferenciar en cuan- to a interfaz y base de datos usada para guardar la información. Son susceptibles a *hackers*, ataques al servidor y son dependientes de la disponibilidad de ese servidor para un correcto funcionamiento.

La tecnología *blockchain* tiene tantas ventajas como la certificación y los *software* de tra- zabilidad, ya que puede usar ambos; el uso de la tecnología *blockchain* no limita el uso de certificaciones, y si instala un nodo en un servidor y este pasa a formar parte de la red *peer- to-peer*, gana todas las ventajas de usar un servidor central, con el extra de seguridad añadida e información real no solo a quien accede al servidor, sino a todos los miembros de la red. La

base de datos replicada garantiza, además, una copia de seguridad en cada participante y la creación de contratos inteligentes permite el desarrollo de *software* sobre esta tecnología. La principal desventaja que presenta es la resistencia al cambio y la curva de aprendizaje, mien- tras el uso de *software* con servidor central lleva un tiempo siendo perfeccionado; una tecno- logía disruptiva como *blockchain* requiere tiempo para consolidarse.

EvoLución de Los contratos inteLigentes

Los contratos inteligentes en *blockchain* evolucionan a aplicaciones descentralizadas, líneas de código que ejecutan procesos de cualquier tipo. En la prueba de concepto realizada en este artículo se demuestra una de las muchas funciones que se pueden programar; estas pueden volverse tan complejas como sean necesarias para resolver problemáticas de cualquier tipo, con las ventajas mencionadas anteriormente.

Un caso de estudio exitoso en la cadena de suministros de alimentos usando Hyperled- gerFabric es conducido por Walmart con apoyo de IBM. En este caso de estudiose llevaron a cabo dos proyectos de prueba de concepto. Un proyecto trataba de rastrear los mangos ven- didos en las tiendas de Walmart en EE. UU. y el otro tenía como objetivo rastrear la carne de cerdo vendida en sus tiendas de China. El sistema de trazabilidad de alimentos basado en *blockchain* de HyperledgerFabric creado para ambos productos funcionó. Para carne de cer- do en China permitió subir certificados de autenticidad a la cadena de bloques, trayendo más confianza a un sistema donde eso solía ser un problema serio. Y para los mangos en EE. UU., el tiempo necesario para rastrear la procedencia pasó de 7 días a 2,2 segundos. A partir de esta prueba de concepto, Walmart ha podido rastrear el origen de más de 25 productos de cinco proveedores diferentes, utilizando un sistema impulsado por Hyperledger Fabric (Hyperled- ger Foundation, s/f).

CONCLUSIONES

La logística internacional está en constante desarrollo y es necesario la implementación de nuevos sistemas que contribuyan a la eficiencia y el correcto funcionamiento de la gestión de la cadena de suministros. La tecnología *blockchain* tiene ventajas que pueden garantizar una reducción de costos, eficiencia y mejor manejo de la información, así como trazabilidad y rastreabilidad en la cadena. La implementación de una plataforma *blockchain* como *software* usado para dar información en tiempo real a todos los actores presentes en la cadena de sumi- nistros, presenta un reto como nuevo mecanismo de transparencia y necesidad de actualiza- ción en el entorno cubano, pero puede solucionar problemas básicos como la estandarización y la necesidad de trazar y rastrear productos en las empresas.

La prueba de concepto creada se hizo utilizando *blockchain* pública, Ethereum. En futuras

investigaciones se recomienda el uso de una *blockchain* privada, como por ejemplo Hyperled- ger Fabric o Alastria, dado que se van a gestionar datos sensibles y se debe dotar al sistema de mayor confiabilidad y seguridad.

AGRADECIMIENTOS

Se agradece a la Empresa de Servicios Técnicos y Logística especializada del tabaco, en parti- cular al director de la UEB Comercial Agrícola, por el apoyo brindado para realizar el estudio de caso y prueba de concepto en su organización.

REFERENCIAS

Ayyildiz, E., & Taskin Gumus, A. (2021). Interval-valued Pythagorean fuzzy AHP method-ba- sed supplychain performance evaluation by a new extension of SCOR model: SCOR 4.0. *Complex & Intelligent Systems, 7*(1), 559-576.

Balcik, B., & Beamon B. M. (2008) Facility location in humanitarian relief, International Jour- nal of Logistics, 11(2), 101-121, http://doi.org/ 10.1080/13675560701561789.

Brakeville, S., & Perepa, B. (2016). Blockchain basics: Introduction to distributed ledgers. *Int. Bus. Mach*, 6, 23-52.

Delgado-Fernández, T. (2021). Taxonomía de Transformación Digital. *Revista Cubana De Transformación Digital, 1*(1), 4–23. https://rctd.uic.cu/rctd/article/view/62.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling block- chain: A data processing view of blockchain systems. *IEEE transactions on knowledge and data engineering, 30*(7), 1366-1385.

Cachin, C., &Vukolić, M., Blockchain Consensus Protocols in the Wild (2017), obtenido el 11 de octubre de 2021. Disponible en: https://arxiv.org/abs/1707.01873v2

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Be- yond bitcoin. *AppliedInnovation, 2*(6-10), 71.

Gereffi, G. (2001). Las cadenas productivas como marco analítico para la globalización. Pro- blemas del Desarrollo. *Revista Latinoamericana de Economía, 32*(125). http://dx.doi. org/10.22201/iiec.20078951e.2001.125.7389

Groenfeldt, Tom. IBM and maersk apply blockchain to container shipping. (En línea) For- bes 2017. Disponible en: https://www. forbes. com/sites/tomgroenfeldt/2017/03/05/ ibm-and-maersk-apply-blockchainto-container-shipping.

Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: trick or treat?. In Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. *Proceedings of the Hamburg International Conference of Logistics (HICL), 23* (pp. 3-18). Berlin: epubli GmbH.

Hyperledger Foundation, (s/f). How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric. Accedido en Agosto 2022.

McKinsey. (2017). Blockchain Technology in the Insurance Sector. En *Proceedings of the Quar- terly Meeting of the Federal Advisory Committee on Insurance (FACI)*. New York, NY, USA: McKinsey & Company.

Monleón-Durá, A. (2020). *Sistema de trazabilidad para cadenas de suministro con blockchain en un entorno empresarial* (Doctoral dissertation, Universitat Politècnica de València).

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review,* 21260.

Song, L., Luo, Y., Chang, Z., Jin, C., Nicolas, M. (2022). blockchain Adoption in Agricultural Supply Chain for Better Sustainability: A Game Theory Perspective. *Sustainability 2022, 14,* 1470. https:// doi.org/10.3390/ su14031470

Steinmetz, R., & Wehrle, K. (Eds.). (2005). Peer-to-peer systems and applications (Vol. 3485). Springer.

Ramírez, J. P. V. (2019). Contratos inteligentes. *Revista de Investigación en Tecnologías de la Información: RITI*, 7(14), 1-10.https://doi.org/10.36825/RITI.07.14.001.

Tiwari, H., & Asawa, K. (2012). A secure and efficient cryptographic hash function based on NewFORK-256. *Egyptian Informatics Journal*, 13(3), 199-208.https://doi.org/10.1016/j. eij.2012.08.003.

Yeow, K., Gani, A., Ahmad, R. W., Rodrigues, J. J., & Ko, K. (2017). Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. IEEE Access, 6, 1513-1524.https:// doi.org/10.1109/ ACCESS.2017.2779263.

Wu, K., Ma, Y., Huang, G., & Liu, X. (2021). A first look at blockchainbased decentralized appli- cations. Software: Practice and Experience, 51(10), 2033-2050. https://doi.org// 10.1002/ spe.2751.