Contratos Inteligentes para Internet de las Cosas

Jorge Eterovic; Marcelo Cipriano; Luis Torres; Dalma Agostina Lomoro

Instituto de Investigación en Ciencia y Tecnología
Dirección de Investigación Vicerrectorado de Investigación y Desarrollo.
Universidad del Salvador.
Lavalle 1854 – C1051AAB -Ciudad Autónoma de Buenos Aires - Argentina

{jorge.eterovic; cipriano1.618 }@gmail.com; torreslu@ar.ibm.com; agostina.lomoro@usal.edu.ar

RESUMEN

Internet de las Cosas (IoT) es un concepto que se refiere a interconectar distintos dispositivos a través de Internet, lo que puede traer muchos beneficios a la sociedad de diferentes maneras. Como los dispositivos están conectados en diferentes contextos y dominios, la información que se genera y se transmite involucra a múltiples partes interesadas.

Esta información puede variar desde lo privado y confidencial hasta lo público, por lo que es muy importante investigar y proponer soluciones para asegurar la integridad de origen, la seguridad y la interoperabilidad. Esto constituye un gran desafío.

En este trabajo de investigación se discute cómo los contratos inteligentes (Smart Contracts) y la tecnología de la cadena de bloques (Blockchain) pueden, potencialmente, llegar a ser una solución viable, aunque todavía no se ha encontrado una manera eficiente y segura para vincular todos los dispositivos de IoT con los contratos inteligentes, ya que no todos los objetos de IoT tienen la potencia computacional necesaria para implementarlo.

El resultado esperado es encontrar soluciones basadas en contratos inteligentes que mejoren la seguridad y la gestión de la información, identificando nuevas oportunidades y desafíos, y brindando recomendaciones y pautas de seguridad para los datos y las comunicaciones de los dispositivos interconectados.

Palabras Clave:
Contratos Inteligentes. Ethereum. Blockchain. Internet de las Cosas.

CONTEXTO

El Vicerrectorado de Investigación y Desarrollo (VRID), perteneciente a la Universidad del Salvador (USAL), dicta las políticas referidas a la investigación, concibiéndola como un servicio a la comunidad y entendiendo que los nuevos conocimientos son la base de los cambios sociales y productivos. Con el impulso de las propias Unidades Académicas se han venido desarrollando acciones conducentes a concretar proyectos de investigación uni/multidisciplinarios, asociándolos a la docencia de grado y postgrado y vinculando este accionar, para potenciarlo, con otras instituciones académicas del ámbito nacional e internacional.

La Dirección de Investigación, dependiente del VRID, brinda soporte a las distintas Unidades de Investigación y a sus investigadores para el desarrollo de Proyectos y Programas de Investigación, nacionales e internacionales, como así también, apoyo y orientación de recursos para la investigación.

A ella pertenece el Instituto de Investigación en Ciencia y Tecnología (RR 576/12) en el cual se enmarca este proyecto denominado “Integración de Blockchain e Internet de las Cosas usando Contratos Inteligentes.”, con una duración de 2 años (2021-2022) y que ya ha sido evaluado y aprobado para su realización.

1. INTRODUCCIÓN

Si buscamos una tecnología que impactará y beneficiará nuestras vidas en los próximos

años, es el Internet de las cosas. Los automóviles, electrodomésticos, teléfonos inteligentes, medidores de servicios públicos, sensores incorporados al cuerpo, indumentaria y casi cualquier cosa que podamos imaginar estarán conectados a Internet y serán accesibles desde cualquier parte del mundo [1]. La revolución que generará IoT será inigualable, algunos autores dicen que será similar a la construcción de carreteras y ferrocarriles que impulsaron la Revolución Industrial de los siglos XVIII al XIX [2], y será transversal a todos los sectores de la sociedad y todas las industrias, desde educación, salud, hogar y ciudad inteligente, hasta manufactura, minería, comercio, logística y vigilancia, solo por mencionar algunas [3].

En Internet de las cosas está involucrada directa o indirectamente la generación de cantidades significativas de información. Un grupo dinámico de partes interesadas debe tener distintos niveles de derechos de acceso a esa información. Además, el alcance de la información relacionada con IoT variará según los requisitos del dominio de la aplicación y el contexto de los dispositivos.

Las aplicaciones de IoT involucran a muchas partes interesadas, con diferentes roles y funcionalidades que acceden a distintos tipos de información con varios niveles de acceso, identidades múltiples y condiciones particulares de seguridad para cada una de ellas. Administrar todos estos activos de manera eficiente, segura e interoperable es un problema desafiante. Se analizará si la tecnología Blockchain y los contratos inteligentes pueden desempeñar un papel importante en este sentido [4].

Una cadena de bloques mantiene una colección, o libro mayor, de transacciones de manera descentralizada y distribuida. El libro mayor es inmutable e irreversible, lo que significa que las transacciones pasadas no pueden ser modificadas por ninguna entidad que registre transacciones en la Blockchain, y se comparte y sincroniza en todos los nodos participantes. De esta manera, la cadena de bloques garantiza que el libro mayor no puede ser manipulado, y que todos los datos que posee la Blockchain son confiables [5].

Una cadena de bloques puede ser pública [6] o estar restringida solo a usuarios autorizados [7]. La Blockchain se considera una forma democrática de mantener transacciones [8] y se prevé que proporcione mecanismos de seguridad novedosos, que contribuyan a la sostenibilidad de las aplicaciones de IoT y permitan nuevos modelos de confianza [9].

Un contrato inteligente es una aplicación distribuida que vive en la cadena de bloques [6]. Esta aplicación es, en esencia, una clase de lenguaje de programación con campos y métodos. Los usuarios pueden interactuar con los campos y métodos públicos de esta clase enviando transacciones a su dirección en la cadena de bloques.

Cada vez que un usuario interactúa con un contrato inteligente, todos los nodos de la red Blockchain ejecutan todas las operaciones de manera determinista y confiable y uno de estos nodos se selecciona para almacenar el resultado de la ejecución de los contratos, si corresponde, en la cadena de bloques. Los contratos inteligentes pueden verificar las identidades y firmas digitales de los usuarios de la Blockchain, realizar cálculos de propósito general e invocar a otros contratos [10].

El código de un contrato inteligente es inmutable y no puede ser modificado ni siquiera por su propietario [11]. Además, todas las transacciones enviadas a un contrato se registran en la cadena de bloques, por lo que es posible obtener todos los valores históricos de una variable del contrato.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

La línea de investigación propone analizar cómo se pueden usar los contratos inteligentes y la tecnología Blockchain para proporcionar mecanismos básicos de seguridad, facilitar la gestión de la información y permitir la interacción con los dispositivos de manera interoperable.

Los contratos inteligentes permiten que las aplicaciones interactúen con los dispositivos de IoT de manera similar a cómo los controladores de hardware permiten que las aplicaciones interactúen con los dispositivos de hardware. Es decir, los contratos inteligentes pueden describir las capacidades de un dispositivo, los servicios que ofrece y cómo se puede acceder a él.

Al escribir los contratos inteligentes, los desarrolladores deberían poder integrar los dispositivos en sus sistemas y procesos, para ofrecer servicios innovadores y sostenibles. Además, al aprovechar los anclajes de confianza proporcionados por los contratos inteligentes y la cadena de bloques subyacente, debería ser más fácil crear aplicaciones distribuidas abiertas, confiables y seguras, así como nuevos mecanismos de seguridad, responsabilidad y cobro. Del mismo modo, con los contratos inteligentes, los usuarios pueden realizar fácilmente transacciones con sus monedas digitales o incluso con sus tokens personalizados.

Una propiedad interesante de los contratos inteligentes es que son deterministas y siempre se ejecutan correctamente, por lo tanto, el propietario de un contrato no debe preocuparse si la lógica de la aplicación, por ejemplo, una condición de control de acceso, incluida en el contrato será respetada o no. Además, el código de un contrato generalmente está disponible y el propietario de un contrato puede incluso agregar controles adicionales en un contrato para proteger a sus clientes. Incluso de sí mismo. Por ejemplo, puede implementar un compromiso de dos fases para los pagos: un cliente, en lugar de pagar directamente a un proveedor de servicios, compromete algo de dinero o activos digitales a un contrato; estos fondos se mantienen en depósito por el contrato hasta que el proveedor de servicios proporcione el servicio esperado; en caso de que no lo haga, los fondos se devuelven al cliente.

Finalmente, los contratos inteligentes no se pueden eliminar de una cadena de bloques. Esta propiedad es útil para construir mecanismos de comunicación resistentes al repudio (non-repudiation). Por ejemplo, y como veremos a continuación, un contrato inteligente puede proporcionar un puntero a la ubicación de un elemento de información, o incluso al elemento en sí. Si esta ubicación se incluye, de alguna manera, en una lista negra, el puntero puede actualizarse fácilmente por el titular del contrato. De manera similar, un contrato inteligente puede contener metadatos que pueden usarse para prevenir fraudes y elementos de contenido falso.

El código fuente del contrato, así como el valor de cada campo del contrato, está disponible públicamente. Por esta razón, los desarrolladores de contratos deben tener mucho cuidado al decidir qué información se almacenará en un contrato. En muchos casos es preferible almacenar los datos fuera de la cadena de bloques y almacenar en la cadena de bloques el hash de los datos. De esta manera, un usuario puede verificar la integridad de los datos recibidos. Además, y por la misma razón, se recomienda a los desarrolladores que utilicen herramientas estáticas (SAST) y dinámicas (DAST) que analicen automáticamente el código del contrato y detecten posibles fallas y riesgos de seguridad [12].

Cabe señalar que cuando decimos que los dispositivos interactúan con una cadena de bloques o con un contrato inteligente, siempre se da a entender que esto es a través de una puerta de enlace confiable. Además, el término usuario puede referirse a entidades del mundo real, aplicaciones, dispositivos o incluso contratos inteligentes.

Se analizan algunos modelos de interacción para IoT basados en contratos inteligentes:

Push-Pull: En este modelo de interacción, los dispositivos hacen que los datos, tanto el contenido como la información, estén disponibles y los empujen (Push) para que los usuarios pueden extraerlos. Para la operación de empuje se pueden considerar los siguientes enfoques:

a) Los dispositivos empujan los datos en la cadena de bloques. Los datos se almacenan en la cadena de bloques, posiblemente a

través de un contrato inteligente. y se pueden usar contratos inteligentes para recuperarlos.

b) Los dispositivos empujan los datos a los nodos de almacenamiento dedicados. Luego almacenan un puntero a ese nodo y los metadatos auxiliares en la cadena de bloques a través de un contrato inteligente. Dependiendo de la forma de este puntero, un usuario puede extraer datos utilizando distintos métodos.

Publish-Subscribe: En este modelo de interacción, los usuarios expresan interés en un elemento de datos (Subscribe) y los dispositivos envían elementos de datos (Publish) a los usuarios interesados. El proceso de suscripción se puede implementar mediante un contrato inteligente, que debe mantener una lista de indicadores para los usuarios interesados. Cada contrato inteligente puede ser responsable de un tema específico y se debe utilizar un mecanismo de resolución para asignar un tema a una dirección determinada de contrato inteligente.

Event-based: Una forma de interacción en el IoT es la actuación (Actuation). Realizar una actuación a través de un contrato inteligente no es trivial, ya que los contratos no interactúan con el mundo físico. Por otro lado, algunas implementaciones de contratos inteligentes proporcionan eventos. Usando eventos, la actuación se puede implementar de la siguiente manera: las operaciones de actuación se pueden implementar como métodos de un contrato inteligente. Los usuarios pueden invocar estos métodos, que a su vez, pueden crear un evento. Los dispositivos podrían monitorear la cadena de bloques en busca de eventos y, si se produce uno, realizarían la actuación adecuada.

3. RESULTADOS OBTENIDOS/ESPERADOS

Como se viene analizando, una de las aplicaciones más importantes de Blockchain que se pueden usar en IoT son los contratos inteligentes.

Los contratos inteligentes son transparentes, se ejecutan de forma determinista por terceros y nadie puede afectar su resultado de ejecución. Proporcionan medios para la autenticación del usuario y la transferencia de tokens. Todas las interacciones con un contrato inteligente se registran en la cadena de bloques. Por otro lado, los contratos inteligentes no son una panacea ya que conllevan riesgos y debilidades. Una vez implementados, no se pueden modificar, no preservan la privacidad del usuario y no pueden almacenar o crear información secreta.

En este trabajo de investigación, se postula que los contratos inteligentes se pueden usar como una abstracción que conectará las aplicaciones con los dispositivos de IoT de una manera eficiente y segura. Unir los dispositivos con contratos inteligentes no siempre será posible, ya que hay dispositivos que no tiene el poder computacional necesario para interactuar con la cadena de bloques.

Además, y teniendo en cuenta que los avances de las investigaciones sobre los protocolos de acceso a los dispositivos y sobre los protocolos de acceso e interoperabilidad de la cadena de bloques avanzan en paralelo, se podría proponer un controlador de protocolos basado en una puerta de enlace (Gateway) que traduciría los protocolos específicos de IoT en transacciones de Blockchain, y viceversa, de manera eficiente y segura.

4. FORMACIÓN DE RECURSOS HUMANOS.

El equipo de investigadores pertenece al cuerpo docente de Tecnologías Aplicadas de la Facultad de Ingeniería, específicamente al área de Seguridad Informática, de la Universidad del Salvador.

A este proyecto, se incorporaron dos docentes investigadores con amplia trayectoria académica, un docente investigador con muchos años de desempeño en la industria de TI y una alumna que se encuentra promediando la carrera de Ingeniería en Informática.

Esto redundará en un aumento del activo académico e investigativo representado por su cuerpo de docentes investigadores, como así también sembrará las bases para la investigación a futuro, a través de la participación de alumnos de la Facultad de Ingeniería.

5. BIBLIOGRAFÍA.

[1] A. Whitmore, A. Agarwal, and L. Da Xu. "The Internet of Things – A survey of topics and trends". Information Systems Frontiers, vol. 17, nro. 2, pp. 261–274. 2015.

[2] Glen Martin (Forbes). "How the Internet of Things Is More Like the Industrial Revolution than the Digital Revolution". https://www.forbes.com/sites/oreillymedia/2014/02/10/more-1876-than-1995/#674c4e0b66d2. Ultima consulta: enero 2022.

[3] L. Da Xu, W. He, and S. Li. "Internet of things in industries: A survey". IEEE Transactions on industrial informatics, vol. 10, nro. 4, pp. 2233–2243. 2014.

[4] M. Conoscenti, A. Vetro, and J. C. De Martin. "Blockchain for the internet of things: A systematic literature review". Computer Systems and Applications (AICCSA), IEEE/ACS 13th International Conference of. IEEE, 2016, pp. 1–6. 2016.

[5] K. Christidis and M. Devetsikiotis. "Blockchains and smart contracts for the internet of things". IEEE Access, vol. 4, pp. 2292–2303. 2016.

[6] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, 2014.

[7] "Hyperledger home page," The Linux Foundation, 2018, (last accessed 23 Feb. 2018). [Online]. Disponible en: https://www.hyperledger.org/

[8] J. Cohn, P. Finn, S. Nair, and P. Sanjai, "Device democracy: Saving the future of the Internet of Things," IBM Institute for Business Value, 2014, Ultima consulta: enero 2022. Disponible en: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03620USEN

[9] G. C. Polyzos and N. Fotiou, "Blockchain-assisted information distribution for the Internet of Things," in Proceedings of the 2017 IEEE International Conference on Information Reuse and Integration, 2017, pp. 75–78.

[10] "Smart contracts, ¿Qué son, cómo funcionan y qué aportan?", Agosto 2016. Disponible en: https://academy.bit2me.com/que-son-los-smart-contracts/. Último acceso: Diciembre 2021.

[11] F. Schüpfer, "Design and Implementation of a Smart Conctract Application", Master Thesis, Agosto 2017. Disponible en: https://files.ifi.uzh.ch/CSG/staff/Rafati/Florian-Schupfer-MA.pdf

[12] K. Christidis and M. Devetsikiotis. "Blockchains and smart contracts for the internet of things". IEEE Access, vol. 4, pp. 2292–2303. 2016.