Aplicación de los Contratos Inteligentes en 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

Blockchain es una de las tecnologías más innovadoras de nuestro tiempo gracias a su capacidad para asegurar la integridad de las transacciones y la autenticidad entre cualquier entidad conectada a Internet, de manera descentralizada. Entre las ventajas que ofrece Blockchain, se incluyen la condición de permamente e inmutable del registro en la cadena de bloques y la capacidad de ejecutar contratos inteligentes.

Internet de las Cosas (IoT) es un concepto que se refiere a interconectar distintos dispositivos a través de Internet, cuestión que puede traer muchos beneficios a la sociedad de diferentes maneras, pero a la vez, es muy importante investigar y proponer la mejor solución para proteger la seguridad de los datos y de las comunicaciones entre todos los dispositivos interconectados. Esto constituye un gran desafío.

Este proyecto de investigación se centra en la búsqueda y análisis de distintas plataformas Blockchain donde se pueden desarrollar contratos inteligentes y mediante ello permiten dar soporte a la interacción entre dispositivos que nos propone el IoT; la recopilación y el estudio de las vulnerabilidades detectadas y cómo es su comportamiento con respecto a la escalabilidad, la complejidad del sistema y los factores del protocolo de consenso.

El resultado esperado es, en el contexto de la integración de contratos inteligentes entre Blockchain e Internet de las Cosas, encontrar las oportunidades y resolver los desafíos de esta integración para proteger la seguridad de los datos y de las comunicaciones garantizando la integridad de las transacciones y un ecosistema seguro para 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 traída por 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 los últimos años, los investigadores han centrado su atención principalmente en abordar los problemas de escalabilidad de las capacidades computacionales y de comunicación de IoT [4]. Si bien estos temas son primordiales para el éxito de IoT y deben investigarse a fondo, la comunidad científica ahora ha reconocido que deben considerarse los problemas de seguridad y privacidad de los datos en IoT, que no tienen precedentes en cuanto a alcance y magnitud y requerirá un considerable esfuerzo de investigación para ser solucionados [5]. Es fácil imaginar que una vez que las personas, los sensores, los automóviles, los robots y los drones puedan interactuar entre sí desde cualquier lugar del mundo, se encontrarán nuevas amenazas y vulnerabilidades que hoy no podemos imaginar.

IoT implementa una arquitectura de acceso centralizado basado en el modelo cliente-servidor en el que las transacciones de IoT (datos, dinero, información en general) entre dispositivos de IoT (sensores, redes de comunicaciones, servidores, aplicaciones, etc.) se realiza con proveedores de servicios monolíticos y centralizados [6]. Este modelo simplifica claramente las interacciones entre los dispositivos de IoT y facilita el proceso de recopilación de datos. Sin embargo, hace que IoT sea vulnerable a una serie de problemas de seguridad y privacidad.

Los proveedores de servicios centralizados pueden hacer un uso ilegítimo de los datos de IoT, como por ejemplo de los sistemas de vigilancia masiva [7]. Aún más importante, los modelos centralizados de recolección de datos pueden exponer a todo el sistema a piratería por actividades maliciosas, con consecuencias nefastas para los ciudadanos, como se dio a conocer en el trabajo de Dan Goodin [8]. Otro desafío importante es la autenticación de los dispositivos de IoT que se conectan a la red [9] Si no se abordan los problemas de autenticación de IoT, los atacantes pueden generar botnets maliciosas, como ya ocurrió con el ataque del malware Mirai [10] y ataques Sybil [11], muy difíciles de detectar.

En un ataque Sybil, un atacante puede contaminar un sistema distribuido creando un gran número de identidades que aparenten ser independientes y usarlas para obtener una influencia desproporcionada, alterar rutas o modificar contenido almacenado de forma redundante. De esta forma, ciertos nodos legítimos pueden sufrir una usurpación de identidad al estar solo conectados a los del atacante. La vulnerabilidad del sistema depende de la facilidad para crear nuevas identidades y la falta de una cadena de confianza bien constituida, que pueda hacer que todas las identidades sean tratadas por igual.

Una manera de abordar los desafíos antes descriptos es organizar el IoT de manera descentralizada, de modo que ningún dispositivo individual tenga control sobre las transacciones de la red de IoT. La descentralización no solo proporciona seguridad y privacidad por diseño, sino que

también les dará a los usuarios la opción de compartir o vender sus datos de sensores con dispositivos de terceros sin intermediarios. El control descentralizado también implica escalabilidad, lo que ha afectado a Internet de las cosas desde su inicio [12]. El desafío es investigar modelos descentralizados de acceso a datos para el IoT, lo que asegurará que los datos de los usuarios no se confíen a dispositivos o empresas centralizadas, sino que se conviertan en propiedad de los propios usuarios.

Las tecnologías y sistemas basados en el concepto de Blockchain están irrumpiendo en el mercado mundial de criptomonedas y pueden resultar adecuados para lograr los objetivos de seguridad y privacidad de IoT mediante un modelo descentralizado [13]. Aunque los algoritmos y principios de Blockchain se conocen desde los años 70, cuando se desarrollaron los árboles de Merkle [14] y los algoritmos de consenso [15], la primera aplicación práctica de Blockchain se propuso en 2008 como parte de la criptomoneda Bitcoin [16]. Desde entonces, se ha aplicado también a una amplia gama de desarrollos no monetarios, que incluyen logística, gestión de energía, ciudades inteligentes, drones, robots y manufactura industrial.

Una cadena de bloques mantiene una colección (o libro mayor) de transacciones de manera descentralizada y distribuida. El libro mayor es inmutable o 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.

Un algoritmo de consenso, que implica un desafío difícil de resolver y que requiere de importantes recursos informáticos, pero fácil de verificar, llamado prueba de trabajo (PoW: Proof of Work), se utiliza para agregar nuevos bloques en la cadena de bloques (minar), y así establecer una red segura y confiable entre entidades no confiables. Para fines de identificación, los nodos de blockchain pueden optar por emplear claves públicas cambiables para evitar el seguimiento. Se fusionan varias transacciones para formar un bloque que se agrega al libro mayor siguiendo el algoritmo de consenso. Cada bloque incluye el hash del bloque anterior en el libro mayor. Cualquier modificación de una transacción de un bloque puede detectarse fácilmente ya que el hash del bloque posterior no coincidirá.

La combinación de Blockchain e IoT tiene un potencial disruptivo. La cadena de bloques puede ayudar a la consolidación de IoT al proporcionar las siguientes ventajas:

Anonimato. Los dispositivos de IoT pueden participar en la cadena de bloques con una clave pública / privada, que no revela en sí misma la identidad real de su propietario;

Descentralización. Los sistemas centralizados tradicionales requieren que cada transacción se valide a través de una autoridad centralizada, por ejemplo, un banco central, lo que produce un cuello de botella en el rendimiento. Por el contrario, la validación de terceros ya no es necesaria en la cadena de bloques, ya que los algoritmos de consenso mantienen la consistencia de los datos;

No repudio. La cadena de bloques asegura que las transacciones se puedan validar fácilmente; y no se admiten transacciones no válidas: es casi imposible eliminar o revertir las transacciones una vez incluidas en la cadena de bloques.

Aunque la cadena de bloques puede parecer la solución para los problemas de seguridad y privacidad de IoT, todavía hay muchos aspectos a resolver que impiden su aplicación inmediata en la mayoría de las redes actuales de IoT. La mayoría de los algoritmos de consenso utilizados por los sistemas basados en Blockchain no fueron diseñados para ejecutarse en dispositivos con restricciones de capacidad de cómputo, de consumo de energía y con ancho de banda extremadamente estricto, como ocurre en Internet de las Cosas. Es necesario abordar varios desafíos clave, que incluyen: problemas de escalabilidad que

surgen de la necesidad de lograr un consenso entre miles de millones de mineros; altas demandas de cómputo debido al uso de algoritmos de prueba de trabajo; y grandes demoras debido a mecanismos contra el doble gasto, problema que no siempre aplica al IoT.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Si analizamos los sistemas de IoT basados en Blockchain investigados hasta ahora en las publicaciones científicas, podemos dividir los documentos por categorías, cada una con el nombre de las aplicaciones de IoT más comunes disponibles en la actualidad: energía inteligente, ambientes inteligentes, robótica, transporte y cadena de suministro.

Energía inteligente. Este campo ha atraído una atención significativa de la comunidad de IoT en los últimos años. La mayoría de los sistemas de IoT propuestos aprovechan la cadena de bloques para preservar la privacidad de los usuarios junto con su información personal; y proteger el sistema de transacciones maliciosas, como los usuarios que intentan vender o comprar una cantidad irrazonable de energía. Se proponen sistemas de subasta donde los usuarios pueden vender al mejor postor su exceso de energía basada en una subasta definida en un contrato inteligente, eliminando así la necesidad de un moderador externo. También se exploró el uso de Blockchain para reconstruir los patrones actuales de transacciones de energía distribuida para permitir transacciones descentralizadas en tiempo real y contratos inteligentes de comercio de energía utilizando un mecanismo de confianza automático.

Ambientes inteligentes. Los ambientes inteligentes han sido estudiados para entornos industriales, para la asistencia sanitaria inteligente, ciudades y hogares inteligentes. En este contexto, la cadena de bloques se utiliza para garantizar la disponibilidad y la no confiabilidad de los datos detectados recopilados en la naturaleza, por ejemplo, una granja.

Robótica. El trabajo existente en esta área aprovecha la cadena de bloques como un sistema para soportar comunicaciones seguras y confiables de vehículos aéreos no tripulados (UAV: Unmanned Aerial Vehicle). Los UAV necesitan coordinar de manera confiable sus acciones, intercambiar datos y tomar decisiones. Se ha presentado un sistema donde los drones están programados para usar Blockchain para transmitir información de forma segura. Se está investigando el uso de Blockchain para proporcionar seguridad, autonomía y toma de decisiones colectivas en sistemas robóticos haciendo uso de una combinación de Blockchain y almacenamiento en la nube para proteger la integridad de los datos recopilados por los drones.

Transporte. En los últimos años, muchos conceptos de IoT se han utilizado para diseñar sistemas de transporte de próxima generación. El aspecto más prometedor es que los vehículos inteligentes probablemente no estarán tan limitados computacionalmente como otros dispositivos IoT, como las plataformas de sensores. Por lo tanto, Blockchain podría convertirse en un sistema para el intercambio de datos a prueba de manipulaciones entre vehículos inteligentes. Del mismo modo, supervise los datos relacionados con el vehículo, por ejemplo, información de mantenimiento e informes de diagnóstico del vehículo, utilizando Blockchain. Se podría usar Blockchain para diseñar una arquitectura de sistema de transporte inteligente completa, que incluya capas de aplicación, contrato, incentivo, consenso, datos, capa física y de red. La cadena de bloques también se ha aprovechado para implementar sistemas para manejar las claves públicas de los vehículos, y en general compartir datos sin una gestión centralizada de terceros. Se han propuesto sistemas de preservación de la privacidad para compartir información relevante, por ejemplo, accidentes, tráfico entre vehículos, donde los participantes son recompensados con tokens monetarios. También se propusieron sistemas de reputación basados en Blockchain que estima la confiabilidad de los mensajes recibidos.

Cadena de suministro y otros. Se han propuesto algunos sistemas para mejorar la funcionalidad de la fabricación basada en la nube y bajo demanda. Se han presentado marcos de distribución basados en Blockchain para compartir conocimientos y servicios entre empresas.

3. RESULTADOS OBTENIDOS/ESPERADOS

Como se ve en los puntos anteriores, una de las aplicaciones más importantes de Blockchain que se pueden usar en IoT son los Contratos Inteligentes.

Una de las principales ventajas de IoT es su capacidad para permitir comunicaciones autónomas y autodirigidas de máquina a máquina (M2M: Machine to Machine). En este contexto específico, es de suma importancia diseñar mecanismos de gestión de manera que las interacciones se inicien automáticamente de acuerdo a condiciones previamente acordadas; y que no haya necesidad de controlar y verificar individualmente la confiabilidad de cada interacción / comunicación. Con este fin, se ha demostrado que los contratos inteligentes [17] son efectivos para resolver los desafíos anteriores.

Si bien la aplicación de contratos inteligentes para IoT aún se está investigando, los resultados preliminares muestran que varias aplicaciones de IoT se beneficiarían de las tecnologías Blockchain como los contratos inteligentes. Por ejemplo, se han investigado los mecanismos de control de acceso que se basan en contratos inteligentes para regular el acceso a la red IoT. Estos trabajos aprovechan la inmutabilidad de Blockchain para generar una lista de control de acceso en tiempo real que también regula y describe las políticas de acceso a los recursos del dispositivo. Blockchain servirá como la columna vertebral de la confianza digital y la seguridad para las interacciones entre dispositivos.

También se discute la posibilidad de lograr un monitoreo inteligente de la cadena de suministro por medio de contratos inteligentes. No solo se pueden usar contratos inteligentes para regular las transacciones y tarifas relacionadas con los procesos de producción y envío de mercancías, sino que también se pueden usar para realizar un seguimiento de su posición.

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 2021.

[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] S. Tayeb, S. Latifi, and Y. Kim. “A survey on IoT communication and computation frameworks: An industrial perspective”.

Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual. IEEE, pp. 1–6. 2017.

[5] F. Restuccia, S. D'Oro, and T. Melodia. "Securing the internet of things in the age of machine learning and software-defined networking". IEEE Internet of Things Journal. 2018.

[6] M. S. Ali, K. Dolui, and F. Antonelli. "IoT data privacy via blockchains and IPFS". Proceedings of the Seventh International Conference on the Internet of Things. ACM, p. 14. 2017.

[7] Julia Powles (The Guardian). "Internet of things: the greatest mass surveillance infrastructure ever?" https://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance. Ultima consulta: enero 2013.

[8] Dan Goodin, Ars Technica. "9 Baby Monitors Wide Open to Hacks that Expose Users' Most Private Moments". http://tinyurl.com/ya7w43e9. 2015.

[9] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang. "A lightweight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment". Future Generation Computer Systems, vol. 78, pp. 1005–1019. 2018.

[10] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas. "DDoS in the IoT: Mirai and other botnets". Computer, vol. 50, nro. 7, pp. 80–84. 2017.

[11] K. Zhang, X. Liang, R. Lu, and X. Shen. "Sybil attacks and their defenses in the internet of things". IEEE Internet of Things Journal, vol. 1, nro. 5, pp. 372–383. 2014.

[12] M. Gharbieh, H. ElSawy, A. Bader, and M.-S. Alouini. "Spatiotemporal stochastic modeling of iot enabled cellular networks: Scalability and stability analysis". IEEE Transactions on Communications, vol. 65, nro. 8, pp. 3585–3600. 2017.

[13] 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.

[14] R. C. Merkle. "Protocols for public key cryptosystems". Security and Privacy, IEEE Symposium. IEEE, pp. 122–122. 1980.

[15] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. "An overview of blockchain technology: Architecture, consensus, and future trends". 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564. June 2017.

[16] S. Nakamoto. "Bitcoin: A peer-to-peer electronic cash system". 2008.

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