Seguridad en Internet de las Cosas usando soluciones Blockchain

Jorge Eterovic; Marcelo Cipriano; García, Edith; Luis Torres

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; edithxgarcia}@gmail.com, torreslu@ar.ibm.com

RESUMEN

El mayor reto al que se enfrenta la seguridad en IoT (Internet of Things, Internet de las Cosas) proviene de la propia arquitectura del sistema actual, que se basa por completo en un modelo centralizado conocido como cliente/servidor. Todos los dispositivos se identifican, autentican y conectan a través de servidores en la nube.

Con el desarrollo de hogares, ciudades y autos inteligentes, el Internet de las Cosas se ha convertido en un área de rápido crecimiento que, según una estimación de la consultora internacional Gartner, se calcula que para 2023 podría haber una cantidad de más de 20 veces de dispositivos IoT conectados a la red que de plataformas de TI convencionales [1]. Sin embargo, la realidad nos muestra que la mayoría de estos dispositivos presentan vulnerabilidades factibles de ser atacadas con fines maliciosos.

Por lo general, estos dispositivos de IoT tienen una capacidad de procesamiento, almacenamiento y de conexión a la red limitados, lo que los hacen más vulnerables a los ataques que otros dispositivos con mayor capacidad como por ejemplo los teléfonos inteligentes, tabletas o computadoras.

En este proyecto de investigación se analizan los principales problemas de seguridad en IoT y como Blockchain, que es una de las tecnologías más innovadoras de nuestro tiempo y su uso viene ganando interés desde su aparición gracias a su capacidad para asegurar la integridad de las transacciones y la autenticidad entre cualquier entidad conectada a Internet de manera descentralizada, puede ser una solución para resolver algunos de los problemas de seguridad de IoT.

Palabras Clave:
Seguridad en Internet de las Cosas. Blockchain. Seguridad de las Redes. Seguridad de los Datos.

CONTEXTO

El Vicerrectorado de Investigación y Desarrollo (VRID), perteneciente a la Universidad Nacional 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 "Análisis de la seguridad de los datos en Internet de las Cosas usando tecnología Blockchain", con una duración de 2 años (2019-2020).

1. INTRODUCCIÓN

Durante los últimos años, el Internet de las Cosas se ha ido introduciendo gradualmente en nuestras vidas gracias a la alta disponibilidad de sistemas de comunicación inalámbricos [2].

El paradigma de IoT abarca muchos conceptos: dispositivos inteligentes que recopilan datos del entorno, muchas tecnologías diferentes para permitir su conexión, servicios y estándares, y todos los elementos que participan [3,4].

IoT puede traer muchos beneficios a la sociedad de muchas maneras diferentes, pero es muy importante estar atentos para que se encuentre la mejor solución para proteger la privacidad de los datos [5,6]. El gran desafío del IoT es encontrar un entorno de comunicación confiable que garantice la seguridad de los datos transmitidos entre todos los dispositivos conectados [7].

Una de las posibles soluciones podría ser la convergencia entre la tecnología IoT y Blockchain [8].

Blockchain ha sido propuesta por la industria y la comunidad de investigación como una tecnología disruptiva que estaría preparada para desempeñar un papel importante en la gestión, el control y, lo más importante, la seguridad de los dispositivos IoT.

Blockchain puede ser una tecnología clave para proporcionar soluciones de seguridad viables a los desafiantes problemas de seguridad de IoT [9,10]. Con el desarrollo de la cadena de bloques Ethereum, que implementa contratos inteligentes, el espacio de uso potencial de Blockchain se ha vuelto muy importante.

Ethereum se lanzó y se abrió para uso público en julio de 2015. Después, surgieron plataformas de Blockchain de contrato inteligente similares. Entre ellas se incluyen Hyperledger [11], Eris [12], Stellar [13], Ripple [14] y Tendermint [15].

A diferencia de la cadena de bloques de bitcoin, que se usa principalmente para transacciones de moneda digital, la cadena de bloques de Ethereum tiene la capacidad de almacenar registros y, lo que es más importante, ejecutar contratos inteligentes. El término contrato inteligente fue acuñado por Nick Szabo en 1994. Un contrato inteligente es básicamente un protocolo de transacción computarizado que ejecuta los términos del contrato.

Para dar una definición simple, los contratos inteligentes son programas escritos por los usuarios para ser cargados y ejecutados en la cadena de bloques. El lenguaje de programación o scripting para contratos inteligentes se llama Solidity, que es un lenguaje similar a JavaScript.

Ethereum Blockchain usa EVM´s (máquinas virtuales Ethereum), que son básicamente los nodos mineros. Estos nodos son capaces de realizar la ejecución y aplicación de estos programas o contratos inteligentes de manera segura usando criptografía a prueba de manipulaciones de confianza [16].

En el contexto de IoT, se espera que Blockchain basado en contratos inteligentes desempeñe un papel importante en la administración, el control y, lo más importante, la seguridad de los dispositivos [1].

Algunas de las características intrínsecas de Blockchain que pueden ser inmensamente útiles para IoT en general, y para la seguridad de IoT en particular son:

1. Identidad de las cosas.
2. Autenticación de datos e Integridad
3. Autenticación, Autorización y Privacidad.
4. Comunicaciones seguras.

Identidad de las cosas. La IDoT (Identity of Things, identidad de las cosas) para IoT debe abordar una serie de problemas desafiantes de manera eficiente, segura y confiable. El desafío principal se refiere a las relaciones de propiedad e identidad de los dispositivos IoT.

La propiedad de un dispositivo cambia durante la vida útil del mismo, pasando del fabricante al proveedor, distribuidor y usuario [17,18]. La propiedad del usuario de un dispositivo IoT se puede cambiar o revocar, si el dispositivo se revende, se da de baja o ha sido comprometido.

La gestión de los atributos y las relaciones de un dispositivo IoT es otro desafío. Los atributos de un dispositivo pueden incluir fabricante, marca, tipo, número de serie, coordenadas GPS de implementación, ubicación, etc. Además de los atributos, capacidades y características, los dispositivos IoT tienen relaciones. Las relaciones de IoT pueden incluir: dispositivo a humano, dispositivo a dispositivo o dispositivo a servicio. Las relaciones de un dispositivo IoT pueden implementarse, utilizarse, enviarse, venderse, actualizarse, repararse, etc.

Autenticación de datos e integridad. Por seguridad, los datos transmitidos por dispositivos IoT conectados a la red deberían estar firmados criptográficamente por el verdadero remitente, que posee una clave pública y un Globally Unique Identifier (GUID) únicos, para asegurar la autenticación e integridad de los datos transmitidos.

Autenticación, autorización y privacidad. En la actualidad se usan complejos protocolos de autenticación, autorización y administración de dispositivos IoT tales como: Role Based Access Management (RBAC), OAuth 2.0, OpenID, OMA DM y LWM2M.

Comunicaciones seguras. Los protocolos de comunicación de aplicaciones IoT como HTTP, MQTT, CoAP o XMPP, o incluso los protocolos relacionados con el enrutamiento como los de RPL y 6LoWPAN, no son seguros por diseño. Dichos protocolos deben incluirse dentro de otros protocolos de seguridad como DTLS o TLS para aplicaciones de mensajería y para proporcionar una comunicación segura. Por lo tanto, se deben buscar protocolos de seguridad livianos que sean más factibles de usar, considerando los limitados recursos informáticos y de memoria de los dispositivos IoT.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Se analizará cómo Blockchain puede ser una tecnología clave para proporcionar soluciones de seguridad viables a los desafiantes problemas actuales de seguridad de IoT y se propondrán alternativas de seguridad con tecnología Blockchain para los distintos aspectos de seguridad antes analizados: Identidad de las cosas; Autenticación de datos e Integridad; Autenticación, Autorización y Privacidad y Comunicaciones seguras.

Se estudiará si Blockchain tiene la capacidad de resolver estos desafíos de manera fácil, segura y eficiente, basándonos en que la cadena de bloques se ha utilizado ampliamente para proporcionar un registro de identidad confiable y autorizado, para el seguimiento de la propiedad y el monitoreo de productos, bienes y datos.

Se propondrán enfoques como TrustChain [19] para permitir transacciones confiables utilizando Blockchain mientras se mantiene la integridad de las transacciones en un entorno distribuido, ya que Blockchain se puede usar para registrar y dar identidad a dispositivos IoT conectados con un conjunto de atributos y relaciones complejas que se pueden cargar y almacenar en el libro mayor distribuido de Blockchain.

En esa línea de investigación se sabe que Blockchain proporciona una gestión descentralizada y confiable, permitiendo el control y el seguimiento en cada punto de la cadena de suministro y del ciclo de vida de un dispositivo IoT, por lo que se propondrá eliminar la administración y distribución de claves, ya que cada dispositivo IoT tendría un GUID y un par de claves asimétricas únicas cuando se instale y se conecte a la red.

La privacidad de los datos también se puede garantizar mediante el uso de contratos inteligentes que establezcan las reglas de acceso, las condiciones y el tiempo para permitir que ciertos individuos o grupos de usuarios o máquinas posean, controlen o

tengan acceso a los datos en reposo o en tránsito.

Los contratos inteligentes también pueden explicar quién tiene el derecho de actualizar y parchear el software o el hardware de IoT, restablecer el dispositivo IoT, proporcionar nuevos pares de claves, iniciar un servicio o solicitud de reparación y cambiar la propiedad de un dispositivo.

3. RESULTADOS OBTENIDOS/ESPERADOS

Los resultados obtenidos hasta el momento fueron presentados en un artículo aprobado para su publicación en la revista digital ReDDI (Revista Digital del Departamento de Ingeniería), editada por el Departamento de Ingeniería e Investigaciones Tecnológicas (DIIT) de la Universidad Nacional de La Matanza (UNLaM), San Justo, Argentina.

En ese trabajo se hace un análisis de las posibilidades de integración de la tecnología Blockchain con IoT, destacando los desafíos y los beneficios que dicha integración supone. También se presentan las futuras líneas de investigación en la integración de Blockchain con IoT y se deja abierto el interrogante de cómo la combinación de ambas puede proporcionar un entorno más seguro que permita desarrollar nuevos modelos de negocios y aplicaciones distribuidas.

Los objetivos de este proyecto de investigación son:

- Exponer en detalle los conceptos de IoT (Internet de las cosas) y Blockchain y hacer un estudio de su impacto en la sociedad y sus perspectivas de futuro como posibles aplicaciones.
- Hacer un estudio de los artículos de investigación y publicaciones que relacionen estos conceptos, destacando las contribuciones más importantes.
- Analizar la privacidad en el intercambio de datos en las principales tecnologías de IoT y cuáles son las mejores contramedidas para evitar las posibles amenazas.
- Analizar los desafíos y oportunidades de la convergencia entre IoT y la tecnología Blockchain.
- Proponer la convergencia de las tecnologías IoT y Blockchain para aplicaciones seguras.

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 la Seguridad Informática, de la Universidad del Salvador.

A este proyecto, se incorporaron un docente investigador con amplia experiencia en la industria y 2 alumnos que se encuentran 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] Gartner Top 10 Strategic Technology Trends for 2020; 2020. https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/.

[2] F. Mattern and C. Floerkemeier; "From the Internet of Computers to the Internet of Things"; ACM Digital Library; From Active Data Management to Event-Based Systems and More; 2010. http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf.

[3] R. Minerva, A Biru, D. Rotondi; "Towards a definition of the Internet of Things (IoT)"; IEEE Xplore Digital Library; 2015. https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_ Revision1_27MAY15.pdf

[4] Shaddad Abdul-Qawy, P. P. J, E. Magesh, T. Srinivasulu; "The Internet of Things (IoT): An Overview"; Directory of Open Access

Journals; International Journal of Engineering Research and Applications; V.5, N. 12; 2015.

[5] D.Mendez, I. Papapanagiotou, B Yang; "Internet of Things: Survey on Security and Privacy"; Cornell University Library; 2017. https://arxiv.org/abs/1707.01879

[6] J. Granjal, E. Monteiro, J. Sá Silva; "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues"; IEEE Xplore Digital Library; IEEE Communications Surveys & Tutorials, 2015, Volume 17, Number 3; http://0-ieeexplore.ieee.org.cataleg.uoc.edu/ document/7005393

[7] A. Bahga, V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things"; Scientific Research; Vol.9, No.10, October 2016. https://www.scirp.org/Journal/Paper Information.aspx?PaperID=71596

[8] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A Margheri, and V. Sassone; "Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments"; First Italian Conference on Cybersecurity (ITASEC17); Venice, Italy; 2017. http://ceur-ws.org/Vol-1816/paper-15.pdf

[9] G.Zyskind, O. Nathan, A. Sandy Pentland; "Decentralizing Privacy: Using Blockchain to Protect Personal Data"; IEEE Xplore Digital Library; Security and Privacy Workshops (SPW); 2015. http://ieeexplore.ieee.org/ document/ 7163223/

[10] T. Tuan Anh Dinh, R. Liu; "Untangling Blockchain: A Data Processing View of Blockchain Systems"; Cornell University Library; 2017. http://www.comp.nus.edu.sg/ ~ooibc/blockchainsurvey.pdf

[11] Linux-Foundation, Blockchain technologies for business, 2017.
URL https: //www.hyperledger.org/.

[12] C. Kuhlman, What is eris? 2016 edition, 2016. URL https://monax.io/2016/04/03/wtf-is-eris/.

[13] Stellar, Stellar network overview, 2014. URL https://www.stellar.org/developers /guides/get-started/

[14] Ripple, Ripple network, 2013. URL: https://ripple.com/network.

[15] All-In-Bits, Introduction to tendermint, 2017. URL: https://tendermint.com/intro.

[16] K. Christidis, "Blockchains and Smart Contracts for the Internet of Things" IEEE Xplore Digital Library, IEEE Access, Volume 4; 2016. http://0-ieeexplore.ieee.org.cataleg.uoc.edu/document/7467408/

[17] I. Friese, J. Heuer, N. Kong, Challenges from the Identities of Things: Introduction of the Identities of Things discussion group within Kantara initiative, in: 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 1–4. http://dx.doi.org/10.1109/WF-IoT. 2014.6803106.

[18] P.N. Mahalle, B. Anggorojati, N.R. Prasad, R. Prasad, Identity authentication and capability-based access control (iacac) for the internet of things, J. CyberSecur. Mobility 1 (4) (2013) 309–348.

[19] P. Otte, M. de Vos, J. Pouwelse, TrustChain: A Sybil-resistant scalable blockchain, Future Gener. Comput. Syst. 2017. http://dx.doi.org/10.1016/j.future.2017.08.048