Estudio de las propiedades criptológicas de los Tokens No Fungibles Inteligentes para asegurar dispositivos de Internet de las Cosas

Jorge Eterovic; Marcelo Cipriano; Edith Garcia; 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
{marcelo.cipriano; jorge.eterovic; edith.garcia; luisantonio.torres}@usal.edu.ar

DESCRIPCIÓN DE LA LÍNEA DE INVESTIGACIÓN

CONTEXTO

El Vicerrectorado de Investigación y Desarrollo (VRID), 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.
La Dirección de Investigación, dependiente del VRID, brinda soporte a las distintas Unidades de Investigación y a sus investigadores, 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 “Estudio de las propiedades criptológicas de los Tokens No Fungibles Inteligentes para asegurar dispositivos de Internet de las Cosas.”, con una duración de 2 años (2023-2024) y que ya ha sido evaluado y aprobado para su realización

RESUMEN

Internet de las Cosas (IoT) es un concepto que se refiere a interconectar distintos dispositivos a través de Internet. 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. El Token No Fungible (NFT) es una solución creada para permitir representar objetos con cualidades únicas, irrepetibles e indivisibles dentro de una Blockchain. Con esta solución, los dispositivos IoT podrían probar no solo que su hardware es de confianza sino también su software, porque ejecutarían un arranque seguro y llevarían a cabo procesos de autenticación mutua con los propietarios y usuarios.

LINEAS DE I+D / RESULTADOS ESPERADOS

Internet de las cosas es el paradigma en el que cualquier cosa puede interconectarse a través de Internet con la capacidad de interactuar, recopilar, procesar y compartir datos de manera inteligente. El rápido crecimiento en la cantidad de cosas conectadas a Internet ha llevado a la necesidad de buscar soluciones de seguridad. Las tecnologías Blockchain podrían utilizarse con IoT ya que generan una cadena de bloques de datos distribuida y criptográficamente segura, permitiendo la trazabilidad. Esto garantiza la propiedad de los mismos y la privacidad del usuario.

Si un atacante intenta cambiar los datos de un bloque, por ejemplo, los datos capturados por los sensores de un dispositivo IoT, el hash del bloque cambia y los datos del siguiente bloque no coinciden. El atacante tendría que cambiar todos los bloques posteriores de la cadena para no ser detectado.

Los datos en los bloques pueden ser capturados por los dispositivos IoT, así como también datos sobre transacciones y los participantes involucrados en las transacciones, En las blockchain públicas, como Ethereum, los acuerdos entre los participantes se formalizan mediante contratos inteligentes representados por scripts que son validados como parte de las transacciones por el algoritmo de consenso y, por lo tanto, una vez validados, los contratos inteligentes son inviolables como los demás datos registrados en la cadena de bloques.

Un token es la representación digital de un activo en la cadena de bloques, existen dos tipos principales de tokens: fungibles y no fungibles (NFT), según el activo representado. Los tokens fungibles son tokens idénticos e intercambiables, como una moneda. Los tokens no fungibles son tokens únicos y no intercambiables, como instrumentos notariales, que permiten la trazabilidad de posesiones físicas o no físicas únicas, como por ejemplo en el contexto de IoT es la capacidad de acceder a recursos o servicios.

Este proyecto de investigación se centra en la búsqueda, estudio y análisis de distintas posibilidades de combinar los dispositivos de Internet de las cosas con las tecnologías blockchain de Tokens No Fungibles para hacer que los dispositivos IoT sean seguros, desde el punto de vista del hardware y del software, de modo que los datos que proporcionan sean confiables.

FORMACIÓN DE RECURSOS HUMANOS

Los 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. Además de la incorporación de un docente investigador con amplia experiencia en la industria, también se cuenta con la colaboración de una alumna cursante de los últimos años de la carrera de Ingeniería en Informática.

La investigación redundará en un aumento del capital humano, académico y científico plasmado en sus docentes investigadores, sembrando las bases para la investigación a futuro, a través de la participación de alumnos de la Facultad de Ingeniería.

USAL
UNIVERSIDAD DEL SALVADOR