

ESTUDIO DE LAS PROPIEDADES CRIPTOLÓGICAS DE LOS TOKENS NO FUNGIBLES INTELIGENTES PARA ASEGURAR DISPOSITIVOS DE INTERNET DE LAS COSAS

STUDY OF THE CRYPTOLOGICAL PROPERTIES OF SMART NON-FUNGIBLE TOKENS TO SECURE INTERNET OF THINGS DEVICES

Investigadores USAL:

Eterovic, Jorge Esteban (jorge.eterovic@usal.edu.ar); Cipriano, Marcelo José;
García, Edith Noemí; Torres, Luis Antonio

Palabras clave: seguridad en IoT, *blockchain*, tokens no fungibles

Keywords: *IoT Security, Blockchain, Non-Fungible Tokens*

Resumen

El token no fungible (NFT) es una solución creada para permitir representar objetos con cualidades únicas, irrepetibles e indivisibles dentro de una *blockchain*. Es un activo digital que representa objetos del mundo real como arte, música y videos. Se compran y venden en línea con criptomonedas y además se construyen utilizando el mismo tipo de programación, como bitcoin o ethereum. El dinero físico y las criptomonedas son “fungibles”, lo que significa que se pueden intercambiar entre sí. Los NFT tienen códigos de identificación únicos que hacen imposible que se intercambien o que sean iguales entre sí, por lo tanto, son “no fungibles”. Los NFT son únicos en su tipo y permiten al comprador poseer el artículo original, y como contiene una autenticación incorporada, sirve como prueba de propiedad. Los datos únicos de los NFT facilitan la verificación de su propiedad y la transferencia de tokens entre propietarios. El propietario o creador también puede almacenar información específica dentro de ellos. Por ejemplo, los artistas pueden firmar su obra de arte al incluir su firma en los metadatos de una NFT. Un token no fungible inteligente (*Smart NFT*) podría representar dispositivos de internet de las cosas (IoT), que son activos físicos inteligentes, y los identificaría como la utilidad de un usuario. Les asignaría una dirección de cuenta de *blockchain* (BCA) para participar activamente en las transacciones, pudiendo establecer canales de comunicación seguros entre propietarios y usuarios y operar de manera segura. Un *Smart NFT* está vinculado físicamente a su dispositivo IoT mediante el uso de una función física no clonable (PUF), que le permite recuperar su clave privada y su dirección BCA, ya que el dispositivo no la guarda en memoria. 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. Los estados del token podrían rastrear los modos de funcionamiento del dispositivo IoT, establecer canales de comunicación seguros entre un dispositivo y su propietario y usuario, y si se agregan sellos de tiempo se podría registrar la última validación del vínculo entre el token y el dispositivo. Este proyecto de investigación se centra en analizar las posibilidades de asegurar los datos de los dispositivos IoT usando los *Smart NFT*.

Abstract

The Non-Fungible Token (NFT) is a solution created to allow representing objects with unique, unrepeatable, and indivisible qualities within a blockchain. It is a digital asset that represents real-world objects such as art, music, and videos. They are bought and sold online with cryptocurrencies and are also built using the same type of programming as Bitcoin or Ethereum. Physical money and cryptocurrencies are “fungible”, meaning they can be exchanged with each other. NFTs have unique identification codes that make it impossible for them to be exchanged or the same as each other; therefore they are “non-fungible”. NFTs are one of a kind and allow the buyer to own the original item and because it contains built-in authentication, it serves as proof of ownership. The unique data of NFTs makes it easy to verify ownership and transfer tokens between owners. The owner or creator can also store specific information within them. For example, artists can sign their artwork by including their signature in the metadata of an NFT. A Smart Non-Fungible Token (Smart NFT) could represent Internet of Things (IoT) devices, which are smart physical assets, and would identify it as a user’s utility. It would assign a Blockchain Account Address (BCA) to actively participate in transactions, being able to establish secure communication channels between owners and users and operate safely. A Smart NFT is physically linked to your IoT device using a Physical Unclonable Function (PUF) that allows you to retrieve your private key and BCA address, since the device does not store it in memory. With this solution, IoT devices could prove not only that their hardware is trustworthy but also their software, because they would execute a secure boot and carry out mutual authentication processes with owners and users. Token states could track IoT device modes of operation, establish secure communication channels between a device and its owner and user, and adding time stamps could record the last validation of the link between the token and the device. This research project focuses on analyzing the possibilities of securing data from IoT devices using Smart NFTs.