

Almacenamiento y Distribución IPFS

Aula USC Santiago

18 de enero de 2025

Resumen

Este documento describe la práctica realizada sobre el almacenamiento y distribución de archivos utilizando el sistema IPFS (InterPlanetary File System). Se detallan las diferentes partes del sistema involucradas, su implementación y cómo se integran con contratos inteligentes para asegurar la gestión de los archivos.

1. Introducción

En esta práctica se exploran los conceptos fundamentales detrás de IPFS, un sistema de archivos distribuido que permite almacenar y compartir archivos de manera descentralizada. IPFS utiliza un enfoque de direccionamiento por contenido, lo que significa que los archivos se identifican y acceden a través de su hash criptográfico. Además, se integra con contratos inteligentes para gestionar el almacenamiento y la distribución de archivos de manera segura, guardándolos en la *blockchain*.

2. Arquitectura del Sistema

2.1. IPFS

IPFS es un sistema de almacenamiento distribuido que permite la gestión eficiente de grandes volúmenes de datos. La clave de su funcionamiento es el uso de un sistema de direccionamiento basado en contenido, donde cada archivo se identifica por un hash único, lo que asegura la integridad de los datos.

2.2. Contratos Inteligentes

En este proyecto, se emplean contratos inteligentes implementados en la blockchain Ethereum, utilizando la testnet de sepolia, para gestionar el almacenamiento de archivos en IPFS. Los contratos permiten almacenar el hash de los archivos, realizar consultas sobre su estado y activar alertas basadas en los valores de los sensores de entrada que tenemos, siendo estos dos de vibración, un magnético y un PIR.

3. Componentes del Sistema

3.1. Nodo IPFS

El nodo IPFS actúa como la parte central del sistema de almacenamiento. Es responsable de almacenar los archivos y distribuirlos a través de la red de nodos IPFS. Cada archivo subido a la red IPFS se almacena con un hash único que se utiliza para acceder al archivo.

3.2. Contratos Inteligentes en Ethereum

Los contratos inteligentes son utilizados para gestionar el almacenamiento de los archivos en la red IPFS, asegurando la integridad de los datos. En este proyecto, los contratos gestionan los hashes de los archivos y emiten eventos de alerta cuando se detectan ciertas condiciones (por ejemplo, cuando un sensor de pone en alta, se emite la alerta de que ha entrado un intruso), todo esto siendo seguro y veraz ya que está almacenado en la blockchain de ethereum.

3.3. Interacción con Node-RED

Node-RED es una plataforma de desarrollo para aplicaciones de Internet de las Cosas (IoT). En esta práctica, Node-RED se utiliza para recibir los datos de los sensores y realizar la interacción con los contratos inteligentes para activar alertas cuando se detectan ciertos valores.

4. Implementación

En primer lugar, hemos definido las ideas principales del contrato inteligente, siendo estas:

1. La capacidad de gestionar datos IPFS, recibiendo su hash generado por la plataforma *pinata*
2. Una función de comprobación de datos, en caso de que se produzca un valor anómalo en un sensor se produce una alerta al "propietario" de esos sensores (La wallet que ha proporcionado los datos)

Siendo así el contrato inteligente que hemos definido. A parte del contrato inteligente, también hemos necesitado:

4.1. Subida de Archivos a IPFS

El proceso de subir un archivo a IPFS comienza con la obtención de un archivo desde una fuente externa (por ejemplo, un sensor o una base de datos) en este caso es un archivo de texto que se sobrescribe cada vez que llegan unos nuevos datos llamado *test.txt*. Este archivo se sube a IPFS, donde se genera un hash único que representa el contenido del archivo. Este hash se almacena en el contrato inteligente.

4.2. Activación de Alertas

La función de los sensores es detectar condiciones específicas y activar una alerta cuando se cumple una determinada condición. En el contrato inteligente, se verifica el valor de los sensores y, si el valor es igual a 1, se emite un evento de alerta. Este evento es procesado en Node-RED con una función que se está suscribiendo periódicamente al contrato y en caso de que se produzca una alerta avisa al usuario en Node-red. Cabe destacar que esto se podría llevar a un aviso por telegram, correo, sms... pero al ser una práctica, no nos hemos complicado.

5. Conclusiones

El sistema implementado demuestra la capacidad de integrar tecnologías como IPFS y contratos inteligentes en la gestión de archivos y alertas. La combinación de estas tecnologías ofrece una solución escalable y segura para el almacenamiento y la distribución de datos, al tiempo que asegura la integridad de los mismos a través del uso de hashes criptográficos.

6. Contenidos enviados

Los programas utilizados son:

1. El contrato siendo el archivo **intrusión.sol**.
2. El node-red donde se simulan los datos de los sensores.
3. El ejemplo de transacción satisfactoria es la siguiente <https://sepolia.etherscan.io/tx/0x05890a2f3edca9052b7e608a93d910217e21ef88ff61d47266ffd7f38ba84407> y la alerta se puede ver en la siguiente imagen 1:

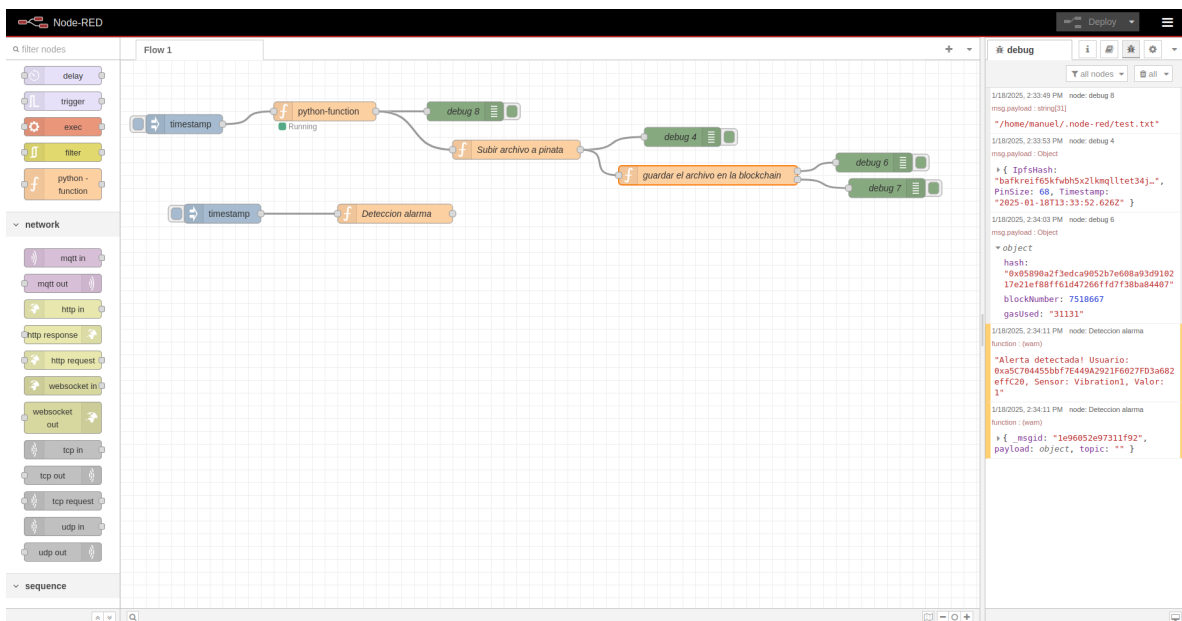


Figura 1: Entorno Node-red con un flujo completado