Tecnologías de Registro Distribuido y Blockchain (BC)

Máster Inter-Universitario en Ciberseguridad (MUNICS)
Universidade da Coruña (UDC) y Universidade de Vigo (UVigo)
Curso 2024-2025

Práctica 2

Alexis Bernárdez Hermida, Nuria Codesido Iglesias

Índice

Caso de uso: Registro y Gestión de Propiedad Intelectual con Blockchain e IPFS

Objetivo del Caso de Uso

Este caso de uso consiste en implementar un sistema descentralizado que permita a los usuarios registrar archivos, transferir derechos de propiedad, verificar autenticidad y gestionar acceso a través de blockchain e IPFS.

Casos de uso

1. **Registro de Propiedad Intelectual.**
   Los usuarios pueden registrar un archivo en IPFS, almacenando el hash, el título y la descripción en la blockchain.

2. **Transferencia de Propiedad.**
   Los usuarios pueden transferir la propiedad de un archivo a otra cuenta de Ethereum. Cada transferencia queda registrada en la blockchain, garantizando así la trazabilidad.

3. **Historial de transferencias.**
   Los usuarios pueden visualizar todas las transacciones realizadas en un archivo registrado en el sistema.

4. **Control de acceso.**
   Permite a los propietarios otorgar permisos de visualización a otros usuarios sin tener que transferir la propiedad del archivo.

5. **Revocar acceso.**
   Permite a los propietarios revocar permisos de visualización a los usuarios.

6. **Licencias Temporales.**
   Los propietarios pueden conceder acceso temporal a sus archivos a otros usuarios. Una vez que este período de tiempo expira, se eliminará dicho acceso.

7. **Verificación de Propiedad.**
   Cualquier usuario puede verificar públicamente si un archivo pertenece a una dirección específica mediante su hash.

8. **Auditoría de Integridad.**
   El sistema permite comprobar que un archivo no ha sido modificado desde su registro, verificando su hash actual con el almacenado.

9. **Registrar disputas.**
   Cualquier usuario puede reportar cualquier conflicto asociado a un archivo registrado en el sistema. Para ello, tiene que especificar el identificador del archivo y el motivo de la disputa.

10. **Visualizar disputas.**
    Cualquier usuario puede visualizar las disputas asociadas a cualquier archivo registrado en el sistema. Para ello, tiene que especificar el identificador del archivo.

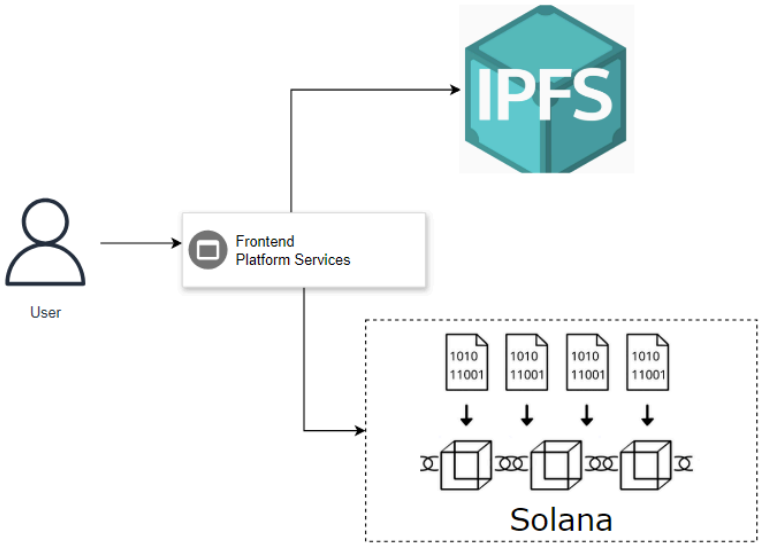
Arquitectura del Sistema

1. **IPFS**.
   Almacena los archivos de los usuarios de manera descentralizada. Su hash se utiliza como identificador único en el sistema.

2. **Blockchain - Solana**.
   Permite ejecutar el contrato inteligente *PropiedadIntelectual* para manejar el registro, transferencia y control de acceso.

3. **Frontend**.
   Es la interfaz de usuario con la que interactúan los usuarios.

4. **Backend**.
   El backend se encarga de gestionar las transacciones en la blockchain y maneja la comunicación entre el frontend y IPFS



Funcionamiento del sistema

Al acceder al sistema, el usuario puede ver cuatro componentes principales: subir archivo, registrar disputas, historial de transferencias y visualizar disputas. A la derecha, se muestran los archivos registrados en el contrato. A continuación, se describen las cuatro funcionalidades a las que puede acceder cualquier usuario:

1. **Registro de Archivo.**
    - El usuario sube un archivo a IPFS seleccionándolo e introduciendo un título y una descripción. Si el usuario aún no está conectado, deberá conectarse a MetaMask antes de poder realizar la carga del archivo.
    - El contrato inteligente registra el hash del archivo, título y descripción en la blockchain.
    - Se genera un token NFT para el propietario.
    - **Errores de Registro**: En el caso de que el archivo ya esté registrado en IPFS, el usuario recibirá un error conforme el archivo ha sido registrado previamente.
    - **Permisos**: Cualquier usuario.

2. **Registrar disputas.**
    - Los usuarios pueden reportar un conflicto asociado a un archivo registrado, indicando el motivo de la disputa.
    - **Permisos**: Cualquier usuario.

3. **Historial de transferencias.**
    - Los usuarios pueden consultar el historial de todas las transacciones de un archivo registrado, permitiendo verificar su propiedad a lo largo del tiempo.
    - **Permisos**: Cualquier usuario.

4. **Visualizar disputas.**
    - Los usuarios pueden consultar las disputas asociadas a un archivo registrado proporcionando el identificador del archivo.
    - **Permisos**: Cualquier usuario.

En caso de que el usuario tenga acceso a un archivo, podrá visualizar su contenido. Además, si el usuario es el propietario, tendrá acceso a funcionalidades adicionales que se describen a continuación.

5. **Transferencia de Propiedad.**
    - El propietario actual ejecuta una transacción en el contrato inteligente indicando el destinatario al que transfiere la propiedad.
    - Se actualiza el historial de transferencias en la blockchain.
    - **Errores**: Si se introduce una dirección inválida, se mostrará un mensaje conforme la address no es válida.
    - **Permisos**: El propietario.

6. **Acceso Controlado y Licencias Temporales.**
    - El propietario concede permisos de visualización usando el contrato inteligente. Además, el propietario puede revocar ese acceso.
    - Las licencias temporales incluyen un período definido que se gestiona automáticamente.
    - **Errores**: Si se introduce una dirección inválida, se mostrará un mensaje conforme la address no es válida.
    - **Permisos**: El propietario.

7. **Auditoría.**
    - El propietario puede verificar si un archivo ha sido alterado, comparando su hash actual con el hash registrado en la blockchain.
    - **Permisos**: El propietario.

8. **Consultar certificado.**
    - El propietario puede consultar el certificado de un archivo mediante su hash almacenado en la blockchain para verificar su propiedad y validez.
    - **Errores**: Si se introduce un hash inválido, se mostrará un mensaje de error al consultar el certificado.
    - **Permisos**: El propietario.

Lecciones Aprendidas

Problemas e Incidencias

1. **Gestión de IPFS:**
    - **Lección aprendida**: La configuración del nodo resultó ser más complicada de lo esperado, pero logramos resolverlo.

2. **Despliegue del Contrato Inteligente:**
    - **Lección aprendida:** Al realizar el despliegue del contrato, olvidamos seleccionar el entorno correcto en "Wallet Connect", lo que generó errores de conexión con la red y dificultó la ejecución de transacciones. La solución fue asegurarnos de seleccionar el entorno adecuado antes de realizar el despliegue para evitar problemas de conexión.

3. **Validar el contrato.**
    - **Lección aprendida**: La validación del contrato a través de Remix presentó algunos desafíos, principalmente con las dependencias de openzeppelin.

Esfuerzo y Tiempo Dedicado

- **Configuración de IPFS y blockchain:** 8 horas.
- **Pruebas en Remix:** 5 horas.
- **Integración frontend-backend:** 20 horas.
- **Pruebas y validaciones:** 4 horas.
- **Documentación:** 3 horas.

Las horas totales en realizar esta tarea entre los dos compañeros, fue de 40 horas aproximadamente.

Conclusión

El proyecto de registro y gestión de propiedad intelectual utilizando blockchain e IPFS, permitió explorar de manera práctica las diferentes ventajas y desafíos que contemplan las tecnologías de registro distribuido. A lo largo del desarrollo de este trabajo, se pudieron destacar algunas lecciones importantes, sobre todo en la importancia de seleccionar el entorno adecuado durante el despliegue del contrato inteligente. La implementación de un sistema descentralizado para registrar archivos, transferir derechos de propiedad a otros usuario y gestionar el acceso, utilizando un contrato inteligente en la blockchain de Solana y el almacenamiento en IPFS, destaca el potencial de estas tecnologías. Principalmente destaca la mejora significativa de la transparencia, ya que todos los archivos registrados son accesibles en la red, optimiza la trazabilidad al poder seguir el historial completo de las transacciones y además garantiza la seguridad, al mantener los datos cifrados.