**Objetivo**

El proyecto tiene como objetivo desarrollar un sistema basado en blockchain que permita a las instituciones educativas emitir certificados estudiantiles únicos tales como la obtención de un título o la aprobación de una materia y que los estudiantes puedan almacenarlos de forma segura en la red. A su vez, el sistema facilitará la verificación pública y transparente de los certificados emitidos, garantizando autenticidad, trazabilidad y resistencia a la falsificación.

**Roles del sistema**

**Admin**: gestiona la lista de instituciones autorizadas para emitir certificados. Se encarga de otorgar o revocar permisos a las cuentas que actuarán como emisores.

**Institución** (Emisor): crea y asigna certificados académicos a los estudiantes. Puede revocar certificados previamente emitidos.

**Estudiante** (Holder): recibe su certificado académico como token soulbound (token intrasferible) y puede compartir su dirección pública para demostrar su validez.

**Verificador**: cualquier tercero (empresa, universidad, organismo) que consulta la blockchain para comprobar la autenticidad y el estado de un certificado.

**Principales casos de uso:**

**Gestionar emisores**

El Admin otorga permisos a una institución para poder emitir certificados.

El Admin puede revocar esos permisos si la institución ya no está autorizada.

**Emitir certificado**

Una institución autorizada emite un certificado académico token soulbound a un estudiante.

El certificado queda registrado en la blockchain con metadatos (título, materia, fecha, hash del documento, etc.).

**Revocar certificado**

La institución que emitió un certificado puede revocarlo en caso de error, fraude o actualización.

El estado del certificado (vigente o revocado) queda disponible en la blockchain.

**Verificar certificado**

Un verificador (empresa, universidad, organismo) consulta en la blockchain si un certificado es válido.

Puede comprobar quién lo emitió, a qué estudiante pertenece y si fue revocado.

**Reglas Clave del Proyecto**

1. **No transferibilidad**

Los certificados son tokens soulbound: una vez emitidos, quedan vinculados de forma permanente a la dirección del estudiante y no pueden transferirse ni venderse.

1. **Emisión restringida**
   * Solo las instituciones autorizadas por el Admin pueden emitir certificados.
   * Ningún usuario sin rol de emisor puede crear certificados.
2. **Revocación controlada**
   * Un certificado puede ser revocado únicamente por la institución que lo emitió.
   * El estado de revocación debe ser visible públicamente.
3. **Metadatos verificables**
   * Cada certificado incluye metadatos (grado, materia, fecha, institución emisora, etc.).
   * El archivo asociado (ejemplo: PDF o imagen del diploma) debe estar almacenado en IPFS (red descentralizada de archivos) y vinculado mediante un hash en la blockchain para garantizar su integridad.
4. **Autenticidad y trazabilidad**
   * Todos los certificados son únicos e identificables en la blockchain.
   * Cualquier tercero puede comprobar quién emitió el certificado y a quién pertenece.
5. **Gestión de permisos**
   * El Admin controla qué instituciones pueden emitir certificados.
   * Los estudiantes no pueden modificarlos ni eliminarlos.
6. **Accesibilidad pública**
   * La verificación de la existencia de certificados debe ser posible sin necesidad de permisos especiales además de la public key del estudiante.