LICDIA
Laboratorio de Investigación en Ciencia de Datos & Inteligencia Artificial

JORNADAS 2026 DE CIENCIA, TECNOLOGÍA Y EXTENSIÓN
DEPARTAMENTO DE CIENCIAS BÁSICAS

Línea de I+D - Blockchain y credenciales

Certificación de logros académicos con blockchain: Diseño y evaluación de un prototipo basado en tokens soulbound

Leonardo Duville[1], David Petrocelli[1] (director)
leoduville@gmail.com · dpetrocelli@unlu.edu.ar
[1] Licenciatura en Sistemas de Información, Departamento de Ciencias Básicas, Universidad Nacional de Luján

Estamos desarrollando y probando un prototipo en blockchain para que la credencial académica sea del estudiante, que no se pueda vender y que quien la reciba pueda comprobar que es auténtica.

1 Problema

En Argentina los títulos digitales ya circulan con firma digital (SIU-Guaraní, SICER), que garantiza su autenticidad. Pero consultar el estado de un título sigue dependiendo de sistemas centralizados, y el estudiante no tiene su credencial en sus manos. Los NFT transferibles tampoco sirven: se pueden vender.

2 Enfoque

Representamos la credencial con un token soulbound (ERC-5484), que no se puede transferir. El estudiante la acepta firmando con su wallet, la institución puede revocarla y, si el estudiante pierde la clave, se reemite.

Tabla 1. Qué se guarda y dónde

En la cadena	token no transferible, hash salado, emisor, fechas y estado (activa o revocada)
Estudiante	JSON de la credencial, salt y su clave privada
Institución	copia del JSON y el salt (para reemitir), clave del emisor y verificación de identidad

No hay datos personales en la cadena. Sin el salt no se puede confirmar el hash probando datos probables (ataque de diccionario); hay una prueba para eso.

3 Cómo se emite una credencial

1 La institución carga los datos y el backend arma el hash salado. →

2 El estudiante firma la aceptación con su wallet (EIP-712). No paga gas. →

3 El backend revisa la firma y envía la transacción. El gas lo paga la institución. →

4 El contrato acuña el token y guarda hash, emisor y estado. →

5 Quien verifica recalcula el hash con el JSON y el salt del estudiante, y lee el estado.

Figura 1. Emisión con aceptación del estudiante. Solo el paso 4 escribe en la cadena. En una reemisión, el contrato revoca el token anterior y acuña el nuevo en la misma transacción.

4 Costo en gas

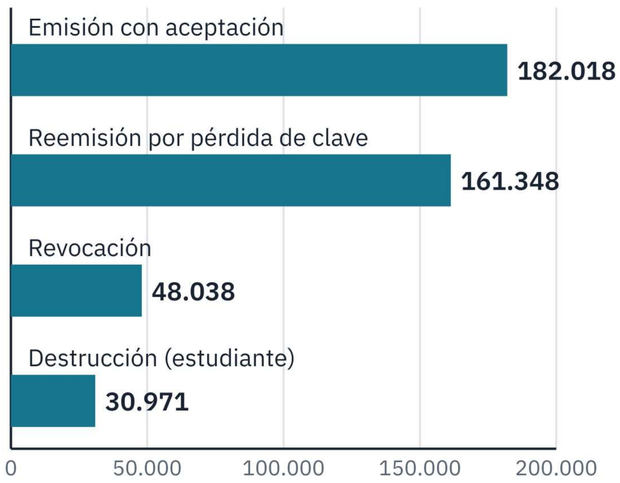

Figura 2. Gas por operación, medido en una red local de pruebas (Hardhat). Revocar cuesta cerca de un cuarto de lo que cuesta emitir. El costo en ETH depende del precio del gas y se va a medir en Sepolia y en Base Sepolia (L2).

5 Qué se probó

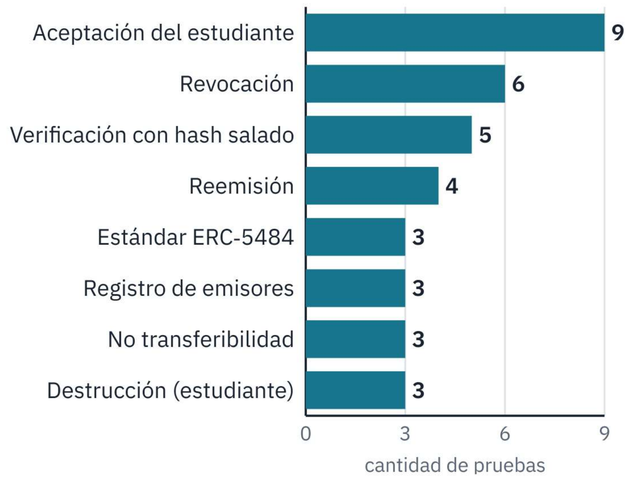

Figura 3. Pruebas automáticas del contrato por propiedad (36 de 37; la restante mide el gas). Pasan las 37 del contrato y las 16 del backend. Sin firma válida no se acuña, una firma reutilizada o vencida se rechaza y la institución no puede destruir la credencial.

6 Conclusiones

El prototipo resuelve la tensión entre no transferibilidad y revocabilidad: la credencial no se transfiere, la institución puede revocarla y el estudiante decide si la acepta y guarda sus datos. Por ahora son resultados de pruebas automáticas; falta mostrar que alguien la usa y que mejora lo que ya existe.

Sigue: desplegar en Sepolia y luego en Base Sepolia (L2), hacer el piloto con 15 a 20 estudiantes (tiempos, gas, adopción y SUS) y completar la comparación con el circuito PKI.

Referencias

1. Weyl et al. Decentralized society: Finding Web3's soul. SSRN, 2022.
2. Wüst y Gervais. Do you need a blockchain? IEEE CVCBT, 2018.
3. Khati et al. Student certificate sharing system using blockchain and NFTs. arXiv, 2023.
4. Belen-Saglam et al. The tension between the GDPR and public blockchain systems. Blockchain: Res. Appl., 2023.
5. Lee et al. A survey on credential revocation and DID deactivation in SSI systems. IEEE Access, 2026.
6. Ley 25.506 de Firma Digital. Boletín Oficial de la República Argentina, 2001.

Líneas de I+D - Investigación aplicada en ciencia de datos e IA, con fuerte impronta en los problemas regionales

Modelos de lenguaje abiertos · IA en educación · Diálogo y RAG · Gobernanza y transformación digital · **Blockchain y credenciales** · Imágenes y datos geoespaciales

licdia.unlu.edu.ar