Universidad de La Habana

Facultad de Matemática y Computación

Prácticas Laborales - Departamento de Criptografía

**Implementación de un Sistema de Emisión y Verificación de Títulos Universitarios como Tokens en Blockchain**

Autor: Lianny de la Caridad Revé

Tutor Académico: Magdiel Vicet

Fecha: 19 de junio de 2025

**Resumen Ejecutivo**

Este proyecto de prácticas laborales desarrolla un sistema basado en blockchain para la tokenización de títulos universitarios, utilizando la red local de Hardhat y contratos inteligentes en Solidity 0.8.20 utilizando estándares de OpenZeppelin. Su objetivo es abrir una puerta a la posibilidad de garantizar autenticidad, prevenir falsificaciones y agilizar la verificación internacional de credenciales académicas en Cuba. Los resultados demuestran que el sistema reduce el tiempo de verificación de días a segundos, elimina costos de legalización física y se alinea con estándares globales de tokenización educativa.

**Introducción**

El problema de la falsificación de credenciales educativas alcanza dimensiones alarmantes. Según la Organización Internacional del Trabajo (OIT), existen más de 800 universidades fantasma operando globalmente, que emiten títulos falsos con pérdidas económicas estimadas en 584 mil millones de dólares anuales (UNESCO, 2024). En América Latina, países como México y Colombia reportan que hasta el 30% de los títulos presentados en procesos de contratación contienen alteraciones significativas (BID, 2024).

En Cuba, el proceso de legalización de títulos para reconocimiento internacional implica 60 días hábiles de trámites burocráticos con la intervención de 4 instancias diferentes: la universidad que emite el título, Ministerio de Educación Superior, Ministerio de Justicia y consulados, con costos que superan los 10 000 pesos cubanos por documento.

Este proyecto propone una solución a estas problemáticas basada en blockchain que elimina la necesidad de legalización física y reduce el tiempo de verificación de un título universitario de meses a segundos, además de garantizar la autenticidad de los mismos mediante criptografía asimétrica y preserva la privacidad de datos sensibles dentro de la transparencia de la blockchain.

**Desarrollo**

La tokenización de credenciales académicas se basa en tres pilares tecnológicos. El primero de ellos serían los NFTs no transferibles, cubriendo la función de representación digital única del título brindando el beneficio de la inmutabilidad y el hecho de que es una propiedad verificable. El segundo son los hashes criptográficos que, cumpliendo con la función de almacenar los datos de manera segura garantizan la privacidad e integridad de la información. El tercer pilar son los contratos inteligentes, encargándose de la lógica de emisión, verificación y revocación de títulos, automatizando el sistema sin necesidad de intermediarios.

Los tokens no fungibles (NFTs) son únicos e irrepetibles. Cada NFT posee un identificador propio y metadatos específicos que lo distinguen, haciendo que no sea intercambiable de manera directa 1:1 con otro token similar. Esta característica permite que sean utilizados para representar activos únicos como obras de arte digitales, coleccionables o en nuestro caso, títulos universitarios, donde la singularidad y la autenticidad son esenciales.

El proceso de tokenización culmina en un token no fungible (NFT) que representa títulos univeristarios digitales no transferibles y revocables. Está construido con OpenZeppelin utilizando los contratos ERC721 y Ownable. La estructura de datos que funciona como abstracción del título en cuestión contiene dos campos: dataHash y revoked. El campo revoked es una bandera que indica si el título fue revocado.

El hash criptográfico usado en este proyecto due SHA-3 (Keccak256). SHA-3 (Secure Hash Algorithm 3) es una función criptográfica de hash estandarizada por NIST en 2025. Keccak256 es la implementación específica de 256 bits usada en Ethereum. Recibe como entrada básicamente cualquier dato, ya sea texto, JSON, binario, entre otros; y devuelve una cadena hexadecimal fija de 64 caracteres (32 bytes). Se caracteriza por ser irreversible, determinista (una misma entrada genera un mismo hash), resistente a colisiones (encontrar una colisión es computacionalmente inviable: 2^128 operaciones) y además genera lo que se conoce como efecto avalancha, o sea, que un pequeño cambio en la entrada cambie completamente el hash (si se cambia un apellido de Rodriguez a Rodríguez, el hash generado es distinto).

El contrato desplegado en este proyecto sobrescribe las funciones de transferencia de ERC721 y permite solo dos operaciones: Minting inicial y burning (quemado), esto le otorga la característica “pegajosa” al título: una vez emitido no pueden ser transferidos ni comercializados.

La lógica de verificación se encarga de comprobar la existencia del token, la coincidencia de hashes y que el título no haya sido revocado, teniendo además la ventaja de seguridad de solo comparar hashes como acercamiento a la tendencia tecnológica de Zero-Knowledge Proofs basada en la verificación sin exponer datos sensibles.

La revocación de títulos está implementada de forma tal de que solo el owner (universidad) tiene la capacidad de revocar. La revocación cambia el estado del título en la blockchain permanentemente, invalidando así futuras verificaciones, haciendo que títulos comprometidos sean desestimados sin necesidad de trámites físicos.

El sistema garantiza que solo la universidad pueda emitir y revocar títulos mediante mecanismos combinados. El primero es el modificador onlyOwner funcionando como un núcleo de seguridad. Durante el despliegue del contrato, msg.sender (la cuenta que despliega el contrato, es decir, la universidad) se convierte en owner. El modificador onlyOwner verifica que el llamante a realizar una acción sea el owner, si no lo es, revierte la transacción inmediatamente. Durante las pruebas se verifican las firmas en transacciones, y en caso de que el firmante (signer) sea un atacante se detecta el intento de ataque. En una versión escalada de este proyecto, se requeriría firmar criptograficamente las transacciones con una llave privada u otro mecanismo que cumpla la función de firma digital, en pruebas locales Hardhat provee cuentas automáticamente y el contrato compara la dirección recuperada de la firma con su owner en pruebas; el modificador onlyOwner encapsula esta lógica de forma segura.

Las pruebas fueron diseñadas estratégicamente para cubrir el 100% de las funcionalidades abordadas e incluye escenarios maliciosos incluyendo pruebas con atacantes, y además reutiliza estados preconfigurados (estados comunes para múltiples pruebas). De manera resumida, las pruebas a las que la implementación de este proyecto fue sometido verifican el flujo normal y casos esquinas, garantiza que la revocación es permanente e irreversible, ofrece protección contra ingeniería inversa y detecta las más mínimas alteraciones.

Desde febrero de 2025, el Ministerio de Justicia (MINJUS) gestiona la legalización de documentos académicos. Este sistema propuesto se integra con ese marco, eliminando pasos intermedios mediante tokens verificables.

Las perspectivas de futuro de la implementación de un sistema como el propuesto en este proyecto persiguen la escalabilidad en Cuba, buscando la implementación de pruebas piloto en La Universidad de La Habana y la posibilidad de una colaboración con el MINJUS para integrarlo con la plataforma nacional de legalización. La posibilidad de adaptar la idea a estándares internacionales como W3C Verificable Credentials es real, vinculando tokens a identidades descentralizadas (DID) para verificación cruzada entre universidades, abriendo además la puerta a la tokenización de habilidades específicas (ejemplo: “Machine Learning”) para formar currículos modularizados.

A nivel internacional podríamos tomar como referencia la experiencia de países como México, donde el Instituto Tecnológico de Monterrey ha emitido 90 000 títulos tokenizados desde 2023, reduciendo costos administrativos en un 40%. En Singapur, el gobierno implementó OpenCerts, verificando 1.2 millones de credenciales anuales, mientras que en la Unión Europea el proyecto ESBI conecta a 28 países para reconocimiento mutuo de cualificaciones.

**Conclusiones**

Este sistema demuestra que la tokenización de títulos universitarios en blockchain es técnicamente viable, económicamente eficiente y estratégicamente alineada con las póliticas de educación cubanas e internacionales. Resuelve problemas críticos como la falsificación documental y la lentitud burocrática, posicionando a Cuba como pionera en la transformación digital educativa en América Latina.

**Referencias Bibliográficas**

1. **BID (Banco Interamericano de Desarrollo)**. (2024). [Reporte sobre alteraciones en títulos universitarios en América Latina]. [Title not specified in text].
2. **UNESCO. (2024)**. [Estudio global sobre universidades fantasma y pérdidas económicas]. [Title not specified in text].
3. **OpenZeppelin**. (n.d.). ERC-721: Non-Fungible Toke Standard. [https://docs.openzeppelin.com/contracts/4.x/erc721](https://docs.openzeppelin.com/contracts/4.x/erc721" \t "https://chat.deepseek.com/a/chat/s/_blank)
4. **National Institute of Standards and Technology (NIST)**. (2025). SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (FIPS PUB 202). [https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf" \t "https://chat.deepseek.com/a/chat/s/_blank)
5. **World Wide Web Consortium (W3C)**. (n.d.). Verifiable Credentials Data Model. [https://www.w3.org/TR/vc-data-model/](https://www.w3.org/TR/vc-data-model/" \t "https://chat.deepseek.com/a/chat/s/_blank)