Proyecto

Sistema de Verificación Distribuida de Certificados Sanitarios mediante Blockchain

Alumno: Israel Jaudy Pérez Bermúdez

Materia: Sistemas Distribuidos y Cómputo en la Nube

Fecha: junio 27, 2025

Maestría en: Ciencias y Tecnologías de Seguridad

Instituto: Instituto Nacional de Astrofísica, Óptica y Electrónica

Índice

Abstract

El presente proyecto desarrolla un sistema distribuido para la verificación de certificados sanitarios utilizando tecnología blockchain y contratos inteligentes. Mediante una arquitectura basada en Ethereum, Ganache y MetaMask, se garantiza la integridad, autenticidad y validez de la información médica sin almacenar datos personales en texto plano. La implementación se realiza a través de una interfaz web ligera conectada a un contrato inteligente escrito en Solidity, que permite emitir, revocar y verificar certificados médicos en formato hash. Además, se complementa con un script en Python para validación descentralizada desde línea de comandos. El sistema simula una red distribuida en entorno local, representando una solución viable y segura ante contextos donde se requiere control de acceso sanitario con criterios de trazabilidad, transparencia y resistencia a manipulaciones.

Palabras clave: Blockchain, Contratos inteligentes, Verificación distribuida, Certificados sanitarios, Web3, Ethereum, Ganache.

1. Introducción

El auge de los sistemas distribuidos ha permitido diseñar soluciones informáticas resilientes, seguras y escalables para el manejo de información crítica en entornos descentralizados. Entre estas tecnologías, blockchain ha destacado por su capacidad para garantizar la inmutabilidad, trazabilidad y disponibilidad de los datos sin requerir de una autoridad central. Esta

característica resulta especialmente valiosa en contextos donde la veracidad de la información y el control de acceso son cruciales, como en los registros sanitarios.

El presente proyecto propone un sistema de verificación distribuida de certificados médicos utilizando contratos inteligentes sobre la red Ethereum. A través de una interfaz web que interactúa directamente con la blockchain mediante MetaMask y la librería `ethers.js`, el ciudadano puede consultar o registrar certificados sanitarios en forma de hash, manteniendo la confidencialidad de la información. Asimismo, se implementa un script en Python para realizar verificaciones automatizadas desde la terminal, permitiendo la integración con otros sistemas o flujos administrativos.

La implementación local con Ganache simula un entorno distribuido controlado que facilita el desarrollo, la depuración y la validación de funcionalidades clave como la emisión, verificación y revocación de certificados. Este enfoque tiene como fin demostrar la viabilidad de una solución ligera, confiable y extensible para el manejo de datos sanitarios en escenarios donde la interoperabilidad y la resistencia a la manipulación son esenciales.

Justificación y contexto sanitario

En situaciones de emergencia sanitaria como la pandemia de COVID-19, se evidenció la necesidad de contar con mecanismos digitales confiables para certificar el estado de salud de los ciudadanos, ya sea en términos de vacunación, pruebas negativas o recuperación médica. Sin embargo, muchos de estos sistemas se basaron en aplicaciones centralizadas con riesgos inherentes a la manipulación de datos, suplantación de identidad o pérdida de integridad documental.

Ante este panorama, un enfoque basado en blockchain permite garantizar que los certificados emitidos no puedan ser alterados y que su verificación pueda realizarse de forma segura por cualquier entidad autorizada. Además, al utilizar hashes criptográficos en lugar de almacenar directamente información personal, se preserva la privacidad del individuo conforme a principios de seguridad por diseño. El presente proyecto se inscribe en esta línea de innovación, proponiendo una solución distribuida, transparente y adaptable a futuros desafíos sanitarios o regulatorios.

2. Objetivos

Objetivo general

Diseñar e implementar un sistema distribuido de verificación de certificados sanitarios utilizando tecnología blockchain, que permita garantizar la autenticación, confidencialidad e integridad de los datos médicos de los ciudadanos, a través del uso de contratos inteligentes, librerías de interacción como `ethers.js`, y mecanismos de control de acceso mediante direcciones públicas de Ethereum.

Objetivos específicos

- Desarrollar un contrato inteligente en Solidity capaz de registrar, verificar y revocar certificados sanitarios codificados como hashes, asociados a una dirección de ciudadano.

- Construir una interfaz web interactiva que permita emitir y verificar certificados mediante MetaMask y la red local de Ganache.
- Implementar un script en Python que verifique desde línea de comandos la validez de un certificado asociado a un hash de documento.
- Simular el funcionamiento distribuido del sistema usando múltiples direcciones simuladas y validaciones desde diferentes contextos de acceso.
- Garantizar que los datos almacenados en blockchain no incluyan información médica sensible en texto plano, preservando la privacidad mediante el uso de hash criptográficos.

3. Desarrollo

El desarrollo del proyecto se basó en una arquitectura distribuida donde se integraron contratos inteligentes escritos en Solidity, una interfaz web basada en HTML y JavaScript, y una simulación de red blockchain con Ganache y MetaMask. A continuación, se detallan las fases técnicas y herramientas utilizadas.

3.1. Diseño del Contrato Inteligente

El contrato fue desarrollado en Solidity y contiene las funciones necesarias para emitir, verificar y revocar certificados sanitarios digitales. Cada certificado está asociado a una dirección pública de Ethereum y guarda la siguiente información: nombre del titular, enfermedad registrada, hash del documento sanitario, y un booleano que indica si el certificado sigue siendo válido. El hash se genera fuera de la blockchain y se utiliza como mecanismo de verificación de integridad [1].

3.2. Configuración de la Red Local

Se utilizó Ganache como blockchain local para simular nodos de Ethereum, configurado con un mnemonic fijo que garantiza persistencia entre sesiones. Además, se implementó un script de despliegue (‘deploy.js‘) usando Hardhat, el cual compila el contrato y lo despliega en la red local. La dirección del contrato se guarda en un archivo de texto para que pueda ser reutilizada por la aplicación web.

3.3. Interfaz Web y Conexión con MetaMask

La interfaz web fue desarrollada en HTML y JavaScript usando la librería `ethers.js` para comunicarse con la red blockchain. Esta interfaz permite:

- Conectar una cartera MetaMask.
- Emitir certificados desde una cuenta autorizada (simulada como autoridad sanitaria).

- Verificar certificados ingresando una dirección pública.
- Revocar certificados previamente emitidos.

El uso de MetaMask simula la interacción entre ciudadanos y autoridades con control de acceso mediante claves públicas [3].

3.4. Verificación por Hash

Para verificar la integridad de los documentos, se implementó un script en Python que usa la librería `web3.py` para consultar los certificados desde blockchain. Este script solicita al usuario una dirección Ethereum, recupera la información del certificado y compara el hash almacenado con uno nuevo generado a partir de un archivo PDF. Si los hashes coinciden y el certificado es válido, se considera auténtico.

3.5. Seguridad y Protección de Datos

Los datos sensibles (nombre y enfermedad) fueron utilizados solo con fines demostrativos. Sin embargo, en un entorno real, estos serían reemplazados por identificadores anónimos o técnicas de cifrado. El uso de hashes asegura que no se expone el contenido del documento directamente en la cadena, respetando principios de confidencialidad y no repudio [2].

3.6. Evidencias del Funcionamiento

Todo el sistema fue probado en un entorno simulado, y su funcionalidad se puede verificar mediante:

- La interfaz web funcional alojada en `http://127.0.0.1:8080`.
- Scripts de verificación y generación de hash funcionales en Linux.
- Repositorio público en GitHub con todo el código fuente y documentación.

4. Resultados

Durante la ejecución del sistema propuesto, se llevaron a cabo múltiples pruebas funcionales para verificar el comportamiento del contrato inteligente, la conexión con MetaMask, y la validación de los certificados sanitarios en la red local de Ganache. A continuación, se presentan las principales evidencias capturadas durante el desarrollo:

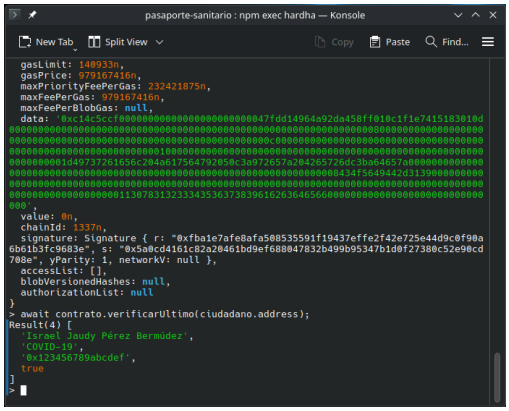

Figura 1: Verificación exitosa en consola de contrato con datos reales en blockchain.

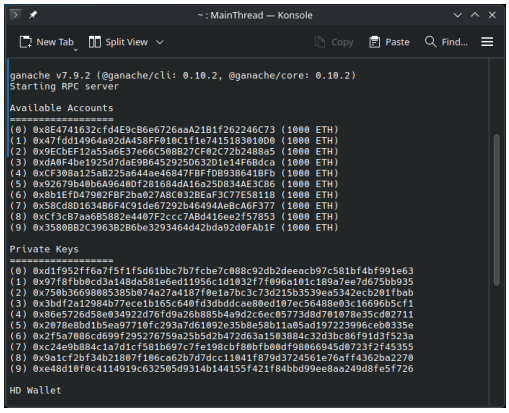

Figura 2: Direcciones y llaves privadas simuladas en Ganache para pruebas distribuidas.

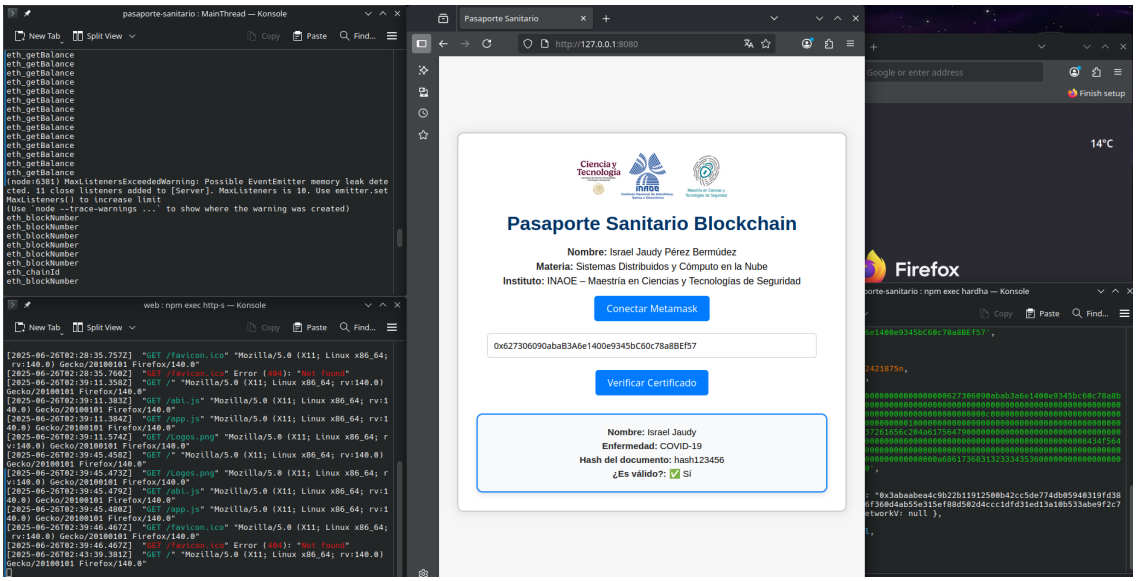

Figura 3: Despliegue local de la aplicación web y pruebas en paralelo con consola y navegador.

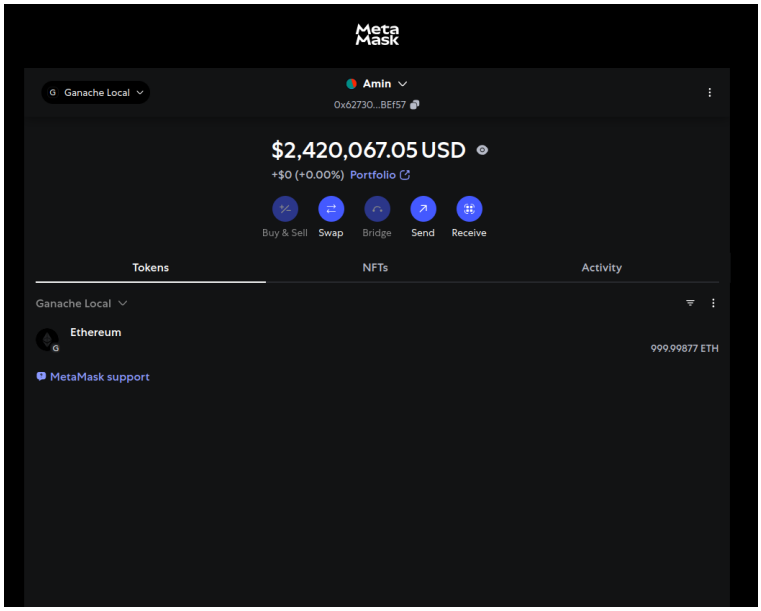

Figura 4: Visualización en MetaMask con fondos simulados en red local.

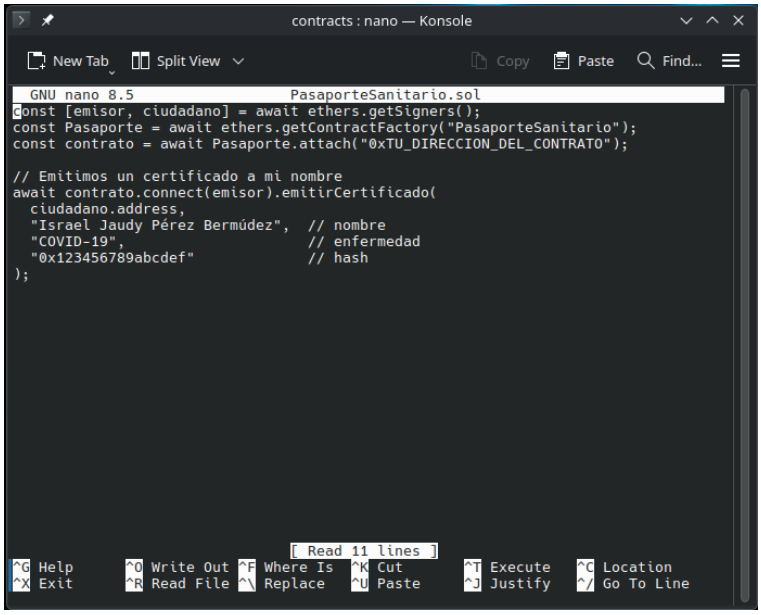

Figura 5: Fragmento de código Solidity con instrucciones de emisión del certificado.

Los resultados demuestran que el sistema logra emitir certificados sanitarios, almacenarlos de forma segura mediante hash en blockchain, y validarlos correctamente desde cualquier nodo autorizado. Además, se integró funcionalidad para revocar certificados previamente emitidos.

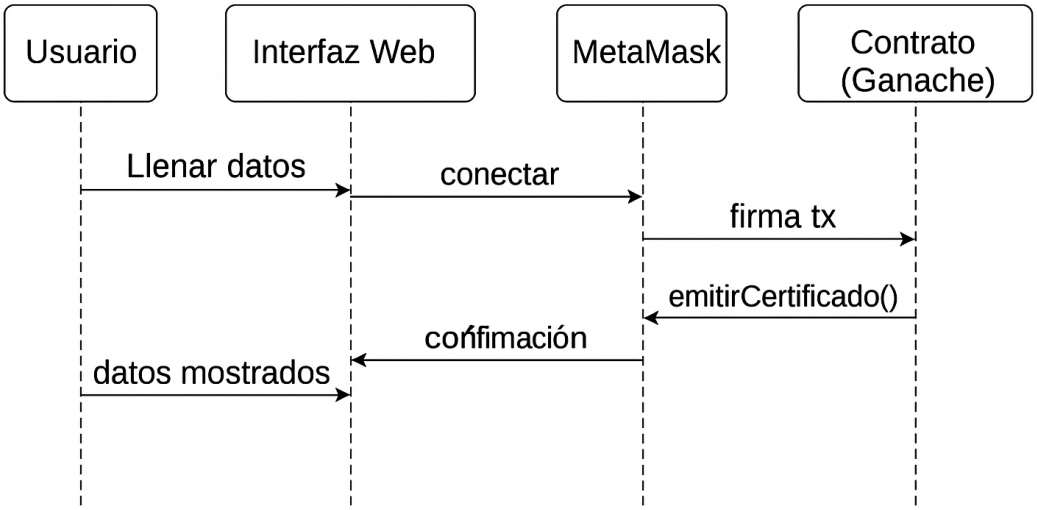

Figura 6: Diagrama espacio-temporal de interacción entre componentes del sistema distribuido.

El diagrama muestra la secuencia de eventos desde que el usuario interactúa con la interfaz web, pasando por la conexión a MetaMask, la emisión del certificado al contrato inteligente desplegado en Ganache y la posterior verificación del mismo. Cada flecha representa una llamada o respuesta entre los componentes, reflejando así la arquitectura lógica de un sistema distribuido respaldado por blockchain.

5. Conclusiones

El presente proyecto demuestra la viabilidad técnica de un sistema distribuido para la emisión y verificación de certificados sanitarios digitales mediante tecnología blockchain. Se logró implementar exitosamente un contrato inteligente en Solidity, capaz de registrar información crítica en forma de hash, garantizar su integridad mediante validación con MetaMask, y desplegar una interfaz funcional accesible a través de la red local.

Se demostró que blockchain puede ofrecer un mecanismo confiable, transparente y resistente a la manipulación para gestionar credenciales sanitarias, todo sin almacenar datos sensibles en texto plano. La verificación de integridad basada en hash y la gestión de permisos mediante direcciones públicas de Ethereum aportan un nivel adicional de seguridad y privacidad.

Además, la experiencia adquirida en el despliegue local con Hardhat, el uso de Ganache y la interacción con Web3 mediante Ethers.js permitió consolidar habilidades prácticas en entornos distribuidos, cumpliendo con los objetivos específicos planteados al inicio del proyecto.

6. Trabajo Futuro

Si bien los resultados fueron satisfactorios, existen oportunidades claras para ampliar y robustecer el sistema propuesto. Entre las tareas a considerar en futuras versiones destacan:

- **Gestión de múltiples usuarios:** Actualmente, el sistema utiliza una sola dirección para simular tanto al emisor como al verificador. Una implementación más avanzada permitiría la interacción entre múltiples actores (ciudadano, entidad de salud, autoridad) con control granular de permisos.
- **Almacenamiento externo del documento:** Aunque se manejan hashes de documentos, no se ha vinculado aún un sistema de almacenamiento descentralizado como IPFS o Swarm. Esto permitiría recuperar el documento original de forma segura y auditable.
- **Firma digital avanzada:** La validación actual se basa en la dirección del emisor. En escenarios reales, sería deseable firmar digitalmente los hashes usando certificados emitidos por una autoridad confiable.
- **Integración con identidad autosoberana (SSI):** El uso de identificadores descentralizados (DIDs) y credenciales verificables puede complementar este modelo, permitiendo mayor privacidad y control por parte del usuario.
- **Despliegue en testnet pública:** Para pruebas más cercanas al entorno real, se sugiere migrar el sistema a una red pública como Goerli o Sepolia, lo que permitirá evaluar costos reales de gas y tiempos de propagación.
- **Hardening de seguridad:** Aunque no se almacenan datos sensibles, es recomendable aplicar revisiones formales de seguridad sobre el contrato inteligente y las interacciones frontend, con el fin de garantizar resistencia ante ataques de reentrancia, desbordamientos u otras vulnerabilidades.

Estas mejoras permitirán transformar el prototipo en una solución robusta y escalable para su posible integración en sistemas de salud o servicios gubernamentales.

7. Referencias

Referencias

[1] Andreas M. Antonopoulos y Gavin Wood. *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media, Inc., 2022.

[2] Arvind Narayanan et al. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[3] Gavin Wood. *Ethereum: A secure decentralised generalised transaction ledger*. Inf. téc. Ethereum Project, 2014. URL: https://ethereum.org/en/whitepaper/.

Repositorio del Proyecto

Este proyecto está disponible públicamente en GitHub. Puedes consultar el código fuente, el contrato inteligente, los scripts en Python y la interfaz web completa en el siguiente enlace:

https://github.com/NullAstra404/Pasaporte-Sanitario

Figura 7: Código QR para acceder al repositorio del proyecto en GitHub.