Seminario Introducción a Blockchain

- **Integrantes:** Bautista Bracco, Aaron Gutierrez
- **Profesores:** Daniel Maximiliano Palazzo, Pablo Sebastian Mosquella Fernandez

VetChain

¿Por qué Blockchain?

VetChain es una aplicación descentralizada (dApp) diseñada para gestionar la identidad, propiedad y trazabilidad médica de animales de compañía. A diferencia de los sistemas tradicionales centralizados (donde cada veterinaria mantiene su propia base de datos), VetChain utiliza tecnología Blockchain para crear una **identidad soberana** para la mascota.

El sistema garantiza que el historial médico sea inmutable, que las transferencias de propiedad cumplan reglas estrictas y que solo profesionales certificados puedan alterar los registros clínicos.

¿Por qué Blockchain?

La Blockchain resuelve problemas fundamentales de confianza y portabilidad de datos:

Inmutabilidad y Confianza

- **Problema:** Un criador o dueño podría falsificar una libreta sanitaria en papel.
- **Solución:** Una vez que un veterinario firma una vacuna en la Blockchain, no es posible borrarla ni alterarla. Esto genera confianza absoluta entre partes que no se conocen.

Identidad Soberana y Portabilidad

- **Problema:** Si cambias de veterinario, tu historial queda atrapado en el software anterior.
- **Solución:** Los datos viven en la red pública, asociados al Chip ID del animal. Cualquier veterinario autorizado puede consultar el historial completo desde cualquier lugar.

Arquitectura de Contratos Inteligentes

El sistema sigue un patrón modular **Controller–Storage** y se integra con un validador externo

ColegioDeVeterinarios (Validador externo)

Este es un contrato desarrollado y mantenido por un tercero que actúa como nuestro **Registro de Autoridades On-Chain**. Su rol es fundamentalmente crítico: **validar la matrícula profesional** de cualquier dirección de *wallet* que intente ejecutar una acción sensible en VetChain.

Esta validación es **esencial** para garantizar que las acciones más críticas de nuestro flujo (como registrar animales o firmar vacunas, que modifican el historial inmutable) sean realizadas **exclusivamente por profesionales legalmente matriculados**.

AnimalNFT (Lógica de Negocio)

Implementa el estándar **ERC-721**, donde cada token representa un animal físico único asociado a su microchip.

¿Por qué ERC-721 para animales?

Elegimos el estándar **ERC-721** porque el **Token No Fungible (NFT)** es el único modelo digital que puede representar la **unicidad inherente** de un ser vivo. Cada mascota es un activo digital **único** (1:1), no intercambiable y no divisible, al igual que un NFT. El token actúa como la **llave de identidad soberana** y el **registro de propiedad verificable** del animal.

Responsabilidades y Decisiones de Implementación

Gestión de Identidad (registerAnimal)

- **Decisión:** Separar el mint del estándar.
- **Motivo:** Solo veterinarios con licencia pueden registrar animales.

Sistema de Permisos (approveVet y _vetApprovalNonce)

- **Decisión:** Usar un Nonce por token en lugar de listas de aprobados.
- **Motivo:** Seguridad y eficiencia. Al transferir un animal, el Nonce se incrementa e invalida permisos previos automáticamente.

Reglas de Transferencia (`_update`):

- **Decisión:** Sobrescribir el hook de transferencia del estándar ERC721..
- **Motivo:** Es el punto de control obligatorio. Acá se consulta a MedicalStorage si la vacuna está vigente y si el animal tiene la edad suficiente (>60 días). Si estas condiciones no se cumplen, la transacción revierte. Esto convierte las reglas de negocio en leyes inquebrantables.

Ventajas

- Validaciones estrictas.
- Reglas de bienestar animal autoejecutables.
- Gestión eficiente de permisos temporales.

Desventajas

- Mayor costo de gas debido a múltiples verificaciones.

MedicalStorage (Almacenamiento)

Funciona como la base de datos del sistema. Solo el contrato **`AnimalNFT`** puede escribir en él.

Responsabilidades y Decisiones de Implementación

Separación de Datos (Storage vs Events)

- **Decisión:** Guardar datos críticos en storage y texto clínico en eventos.
- **Motivo:** Ahorro del 90% en costos de gas.

Lógica de Fechas (vaccineExpiration)

- **Decisión:** Guardar timestamps en vez de booleanos.
- **Motivo:** Permite que el estado sanitario caduque automáticamente.

Control de Acceso (onlyController)

- **Decisión:** Solo `AnimalNFT` puede escribir.
- **Motivo:** Integridad y cumplimiento de reglas de permisos.

Ventajas

- Arquitectura upgradeable.
- Costos de gas optimizados.

Desventajas

- Para leer el historial completo es necesario indexar eventos desde el frontend.

Integraciones Externas y UX

IPFS (Pinata)

- Se utiliza para almacenar archivos pesados como fotos, radiografías y PDFs.
- La blockchain solo guarda el CID.

Firebase (Directorio de Usuarios)

- Mapea emails a direcciones de wallet.
- Permite buscar usuarios por correo sin comprometer la seguridad on-chain.

Conclusión

La arquitectura de VetChain v4 muestra cómo la Blockchain puede transformar la medicina veterinaria. Separar la **lógica de negocio** (AnimalNFT) del **almacenamiento** (MedicalStorage) y apoyarse en **validadores externos** proporciona un sistema seguro, eficiente y transparente.

Código

https://github.com/aarongutierrez08/vetchain-dapp/tree/main