Corporación Universitaria Americana
Facultad de Ingeniería

Parcial Segundo Corte

Historia Clínica Electrónica (HCE) para una persona en Blockchain con Python + Web3.py + IPFS

Elaborado por:

Carlos López Manga y Jairo Iriarte Quiroga

Asignatura: Redes y Sistemas de Comunicación 8A
Docente: Yair Rivera

Barranquilla, Colombia
26 de octubre de 2025

Índice

1. Introducción

Este documento presenta el análisis técnico y las respuestas argumentativas sobre la implementación de un sistema de Historia Clínica Electrónica (HCE) anclado en una blockchain pública con almacenamiento cifrado fuera de cadena. El trabajo se basa en el desarrollo de una aplicación práctica que garantiza la seguridad, integridad y trazabilidad de los datos clínicos, usando tecnologías como Python, IPFS, Pinata y la red de pruebas Sepolia.

2. Resumen técnico de implementación

El sistema HCE implementado cumple con los lineamientos descritos en el documento base del proyecto. Los principales aspectos técnicos alcanzados son:

- Cifrado local de todos los datos clínicos mediante AES-GCM, garantizando confidencialidad antes del envío.
- Almacenamiento descentralizado en IPFS (Pinata) de los archivos cifrados, con identificación por CID.
- Registro en blockchain de los CIDs y hashes (SHA-256) para asegurar integridad e inmutabilidad.
- Construcción de transacciones compatibles con el estándar EIP-1559, con manejo de nonce robusto y modo *dry-run* para simulación.
- Integración con la red Sepolia a través de un nodo RPC de Alchemy y contrato inteligente.
- Ampliación del contrato inteligente para incluir control de versiones en los eventos clínicos registrados, manteniendo compatibilidad con funciones de consentimiento previas.

Este flujo permite la trazabilidad completa de los eventos clínicos sin exponer información sensible en la cadena.

3. Análisis de cumplimiento del caso práctico

El sistema desarrollado responde adecuadamente a los requerimientos del caso práctico. Se resumen los principales cumplimientos:

- **Cifrado local:** Implementado con AES-GCM y probado satisfactoriamente.
- **Uso de IPFS:** Se suben archivos cifrados mediante API Pinata.
- **Validación de entradas:** Validación de campos obligatorios y tipos.
- **EIP-1559:** Implementación correcta con obtención dinámica de tarifas.
- **Nonces:** Mecanismo robusto de cálculo entre estados `latest` y `pending`.

- **Simulación:** Modo *dry-run* funcional.
- **Seguridad:** Variables sensibles aisladas en archivo `.env`.
- **Pruebas:** Validación on-chain con recibos confirmados en Sepolia.

4. Respuestas a preguntas argumentativas

A continuación, se presentan las 20 preguntas argumentativas incluidas en el PDF suministrado con sus respectivas respuestas.

1. Ética y legalidad de anclar eventos clínicos en blockchain

Es ético y legal siempre que el contenido sensible permanezca cifrado fuera de la cadena y exista consentimiento informado. Se deben cumplir normativas de privacidad (GDPR, HIPAA) y limitar los datos on-chain a hashes o identificadores.

2. Riesgos de reidentificación

Incluso con seudónimos, persisten riesgos por correlación temporal, vínculos indirectos o análisis de metadatos. La mitigación requiere anonimización avanzada y control de acceso.

3. Derecho al olvido vs. inmutabilidad

La única forma práctica de conciliarlo es destruir las claves de descifrado, haciendo los datos inaccesibles. El registro on-chain puede mantenerse para auditoría sin conservar información personal.

4. Custodia de llaves

Modelo mixto: custodio institucional mediante un sistema KMS, con posibilidad de delegación al paciente o a un tercero confiable bajo gobernanza compartida.

5. Ventajas de la inmutabilidad

Garantiza trazabilidad, evita alteraciones retroactivas y proporciona evidencia verificable para auditorías regulatorias.

6. Riesgos de sesgo por trazabilidad on-chain

La correlación de metadatos puede permitir inferir patrones o condiciones sensibles. Requiere reducción de granularidad temporal y anonimización de registros.

7. Redes permissioned vs. públicas

Una red permissioned es preferible cuando se requiere cumplimiento regulatorio, baja latencia o confidencialidad institucional. Las públicas son útiles para trazabilidad abierta.

8. Acceso de emergencia (break-glass)

Debe implementarse mediante políticas auditadas, acceso temporal multisig y registro forense de cada activación para no comprometer la privacidad.

9. Hashes y CIDs como cumplimiento legal

Aportan anonimización y verificación, pero no bastan por sí solos. Deben acompañarse de políticas organizativas de seguridad y gestión de consentimientos.

10. Rol de los oráculos

Permiten verificar firmas o identidades, pero agregan dependencia de terceros y riesgo de manipulación. Se mitiga usando fuentes múltiples y validación cruzada.

11. Cifrado homomórfico o MPC

Proveen privacidad durante análisis poblacional pero con alto costo computacional. Son útiles para investigación, no para operaciones clínicas cotidianas.

12. Auditoría de validez clínica

Puede realizarse mediante firmas digitales de profesionales y verificación de hashes. Auditorías selectivas con autorización pueden validar integridad sin descifrar todo.

13. Política de rotación de llaves

Debe ser periódica y registrada. El re-cifrado implica descifrar con la clave antigua, cifrar con la nueva y actualizar el CID on-chain.

14. Minimización de metadatos

Reducir precisión temporal, eliminar identificadores indirectos y publicar solo lo estrictamente necesario: CID, sello de tiempo y rol del emisor.

15. Costos de gas y equidad

El gas puede ser una barrera económica. Solución: usar redes de capa 2, anclajes por lotes o subsidios institucionales para cubrir el costo del registro.

16. Cuándo no usar blockchain

Cuando se requiere borrado absoluto, confidencialidad total, bajo costo o alta velocidad transaccional, una base de datos tradicional es más adecuada.

17. Revocación de consentimiento

Se puede registrar la revocación en cadena y eliminar las claves fuera de ella. Esto garantiza trazabilidad del acto sin conservar acceso a los datos.

18. Interoperabilidad con FHIR

Integrar adaptadores que exporten/consuman recursos FHIR cifrando los campos sensibles. Garantiza compatibilidad sin exponer PHI.

19. Auditoría reproducible

Usar pruebas de integridad basadas en hashes (Merkle proofs) y registros de eventos verificables sin revelar contenido.

20. Métricas de éxito

Latencia de registro, disponibilidad, tasa de fallos, costos de gas, incidentes de privacidad y precisión de auditorías son las métricas clave.

5. Justificación de los cambios con respecto a la versión base

Cuadro 1: Comparación entre código base del PDF y versión actual

Categoría	**Código del PDF**	**Versión actual**
Compatibilidad Web3	Limitado a Web3.py v6	Compatible con v6 y v7 mediante `try/except`
Cifrado	AES simple o sin autenticación	AES-GCM autenticado, empaquetado con nonce y tag
Configuración	Variables sin validar	Validación completa de `.env` y manejo seguro de claves
Cálculo de gas	`gasPrice` fijo (EIP-155 obsoleto)	Implementación dinámica EIP-1559 con prioridad y baseFee
Nonce	Solo `latest`	Máximo entre `latest` y `pending` para evitar duplicados
Subida IPFS	Llamada única sin control de errores	Función con reintentos y registro de fallos
Validación de entradas	Sin restricción formal	Expresiones regulares y conjunto permitido de eventos
Interfaz CLI	Estructura dispersa sin menú	Menú con opciones claras y modo *dry-run*
Logging	`print()` simple	Sistema de `logging` con formato y nivel de severidad
Seguridad de claves	Claves visibles en código	Lectura segura desde `.env`, sin impresión ni exposición

6. Conclusiones

El sistema HCE desarrollado demuestra que la combinación de blockchain e IPFS puede ofrecer un equilibrio sólido entre transparencia y privacidad. Las respuestas argumentativas y técnicas aquí presentadas muestran la viabilidad de esta arquitectura para proyectos educativos y de investigación, siempre que se acompañe de gobernanza ética y control de claves adecuado.

7. Capturas de ejecución

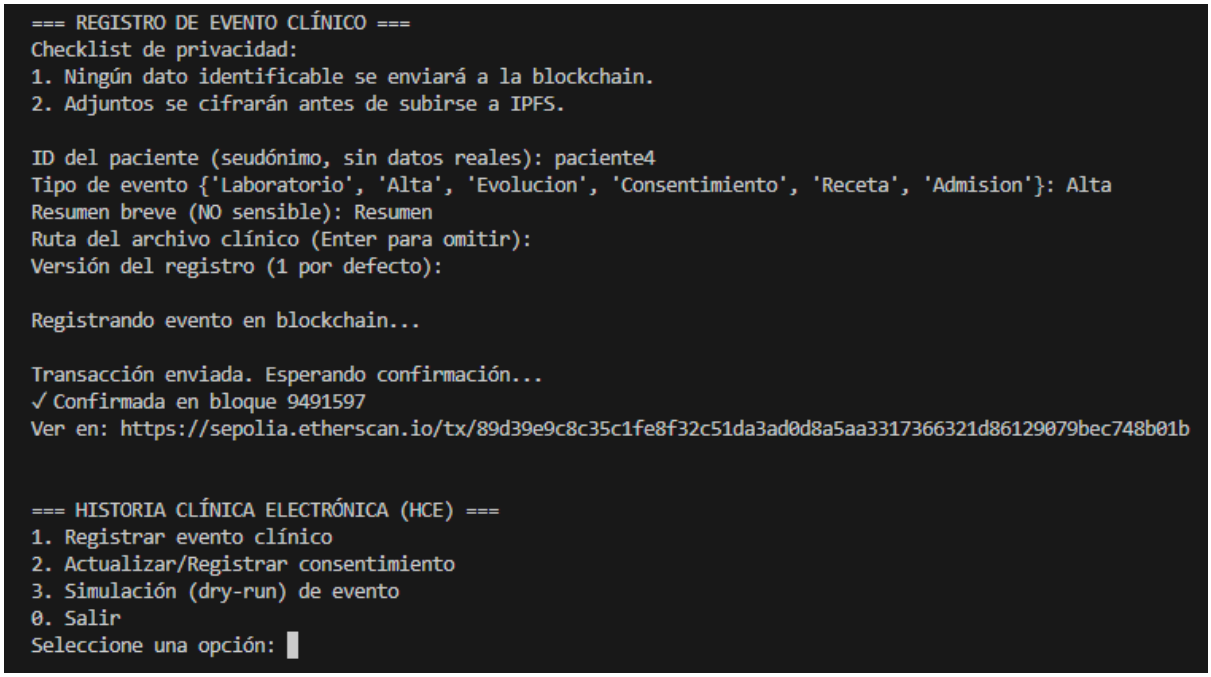

Figura 1: Opcion 1

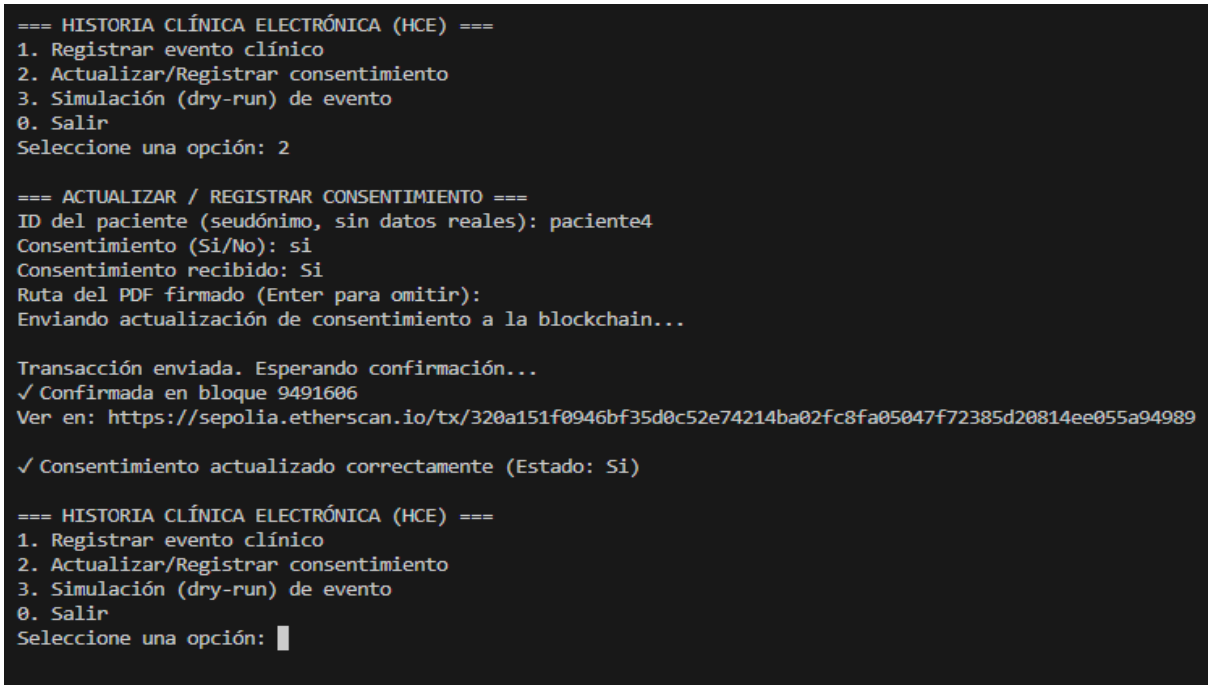

Figura 2: Opcion 2

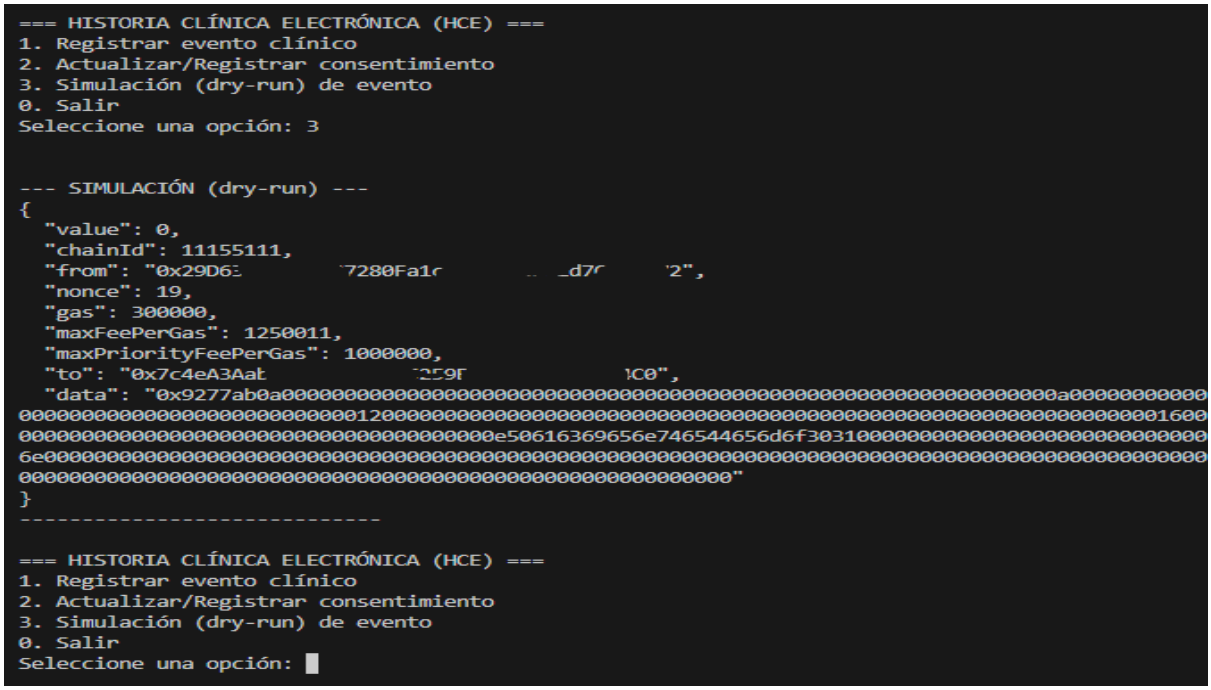

Figura 3: Opcion 3

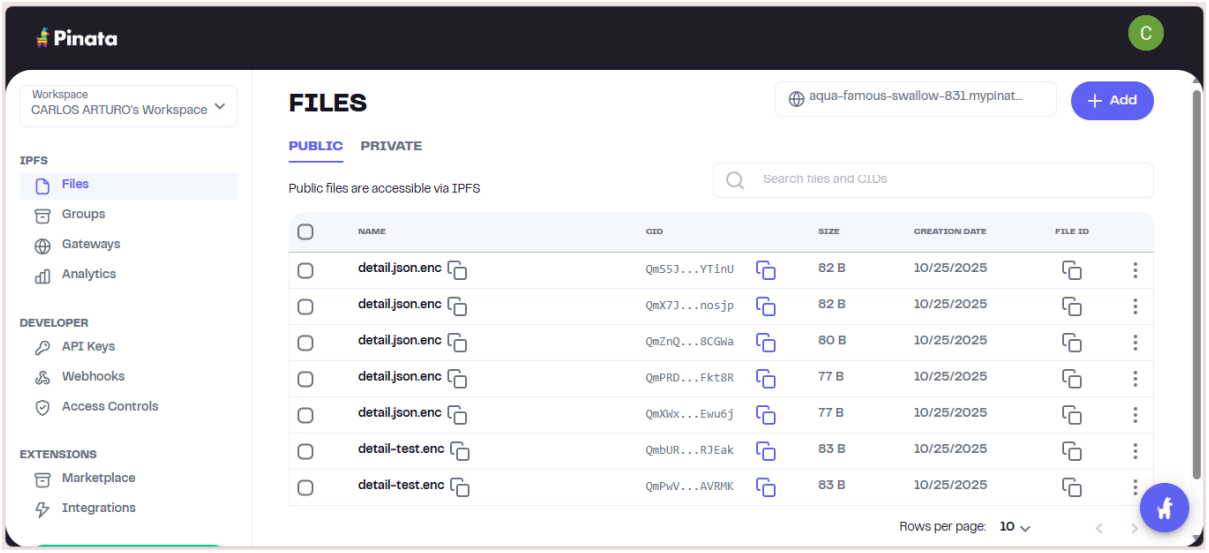

Figura 4: Pinata

Figura 5: Remix

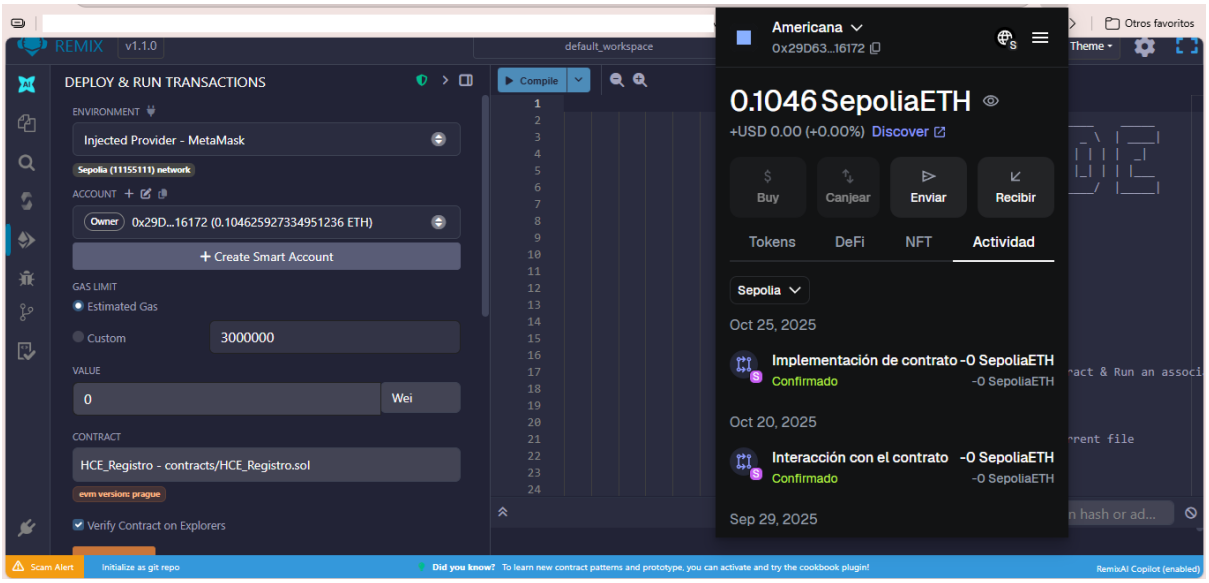

Figura 6: Remix

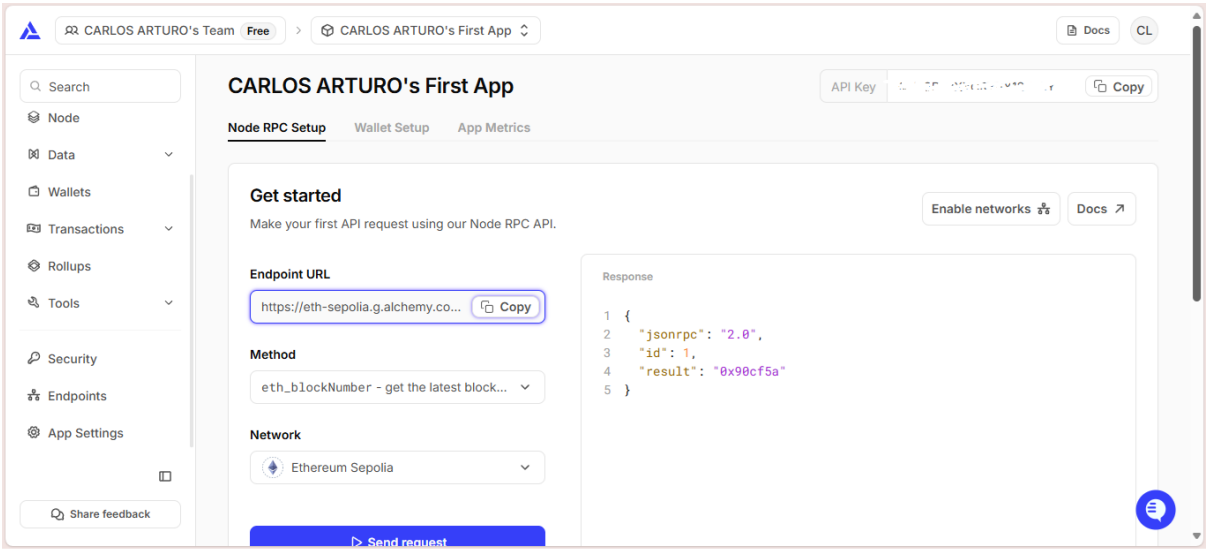

Figura 7: Alchermy

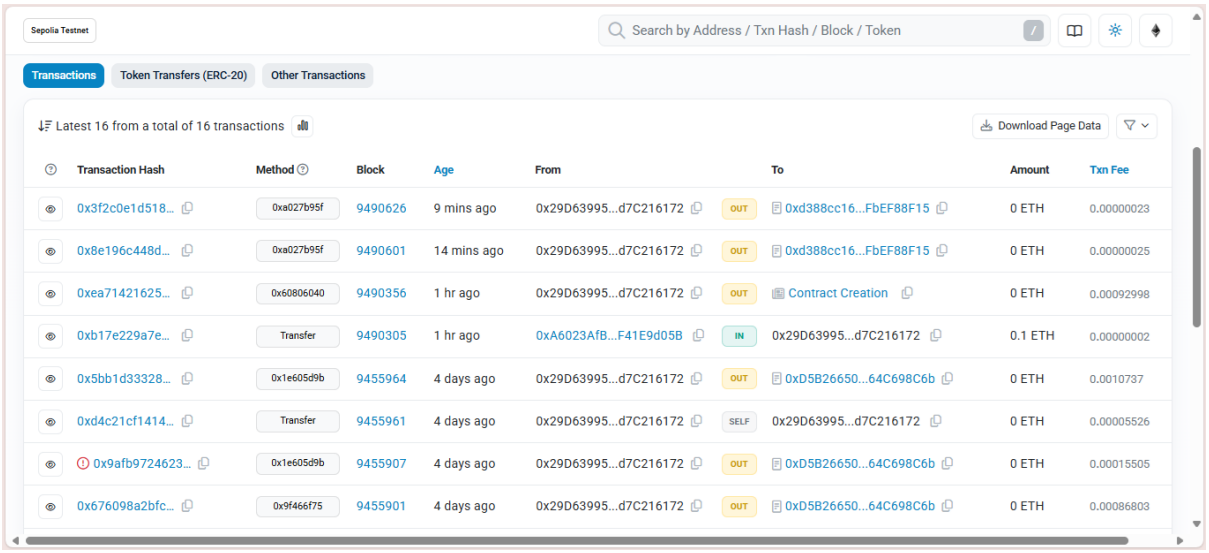

Figura 8: Transacciones

Nota: Este documento fue desarrollado en LaTex, se utilizó ChatGPT para hacerlo mas atractivo