ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

DISEÑO Y PROTOTIPO DE UN SISTEMA DE AUDITORÍA Y CONTROL ELECTORAL PARA LOS PROCESOS DE ESCRUTINIOS Y PUBLICACIÓN DE RESULTADOS BASADO EN DLT

ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DEL PROTOTIPO DEL SISTEMA DE CADENA DE BLOQUES (INFRAESTRUCTURA, CONTRATOS INTELIGENTES Y APLICACIÓN)

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN CIENCIAS DE LA COMPUTACIÓN

CHRISTIAN GABRIEL SATAMA MORALES

christian.satama@epn.edu.ec

DIRECTOR: LUIS ENRIQUE MAFLA GALLEGOS

enrique.mafla@epn.edu.ec

QUITO, JULIO 2024

CERTIFICACIONES

Yo, CHRISTIAN GABRIEL SATAMA MORALES declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

_____

CHRISTIAN GABRIEL SATAMA MORALES

Certifico que el presente trabajo de integración curricular fue desarrollado por CHRISTIAN GABRIEL SATAMA MORALES, bajo mi supervisión.

_____

LUIS ENRIQUE MAFLA GALLEGOS

DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

CHRISTIAN GABRIEL SATAMA MORALES

LUIS ENRIQUE MAFLA GALLEGOS

ANDRES EDUARDO ARMENDÁRIZ BASTIDAS

EMERSON RICARDO CERACAPA SOLÍS

ÍNDICE DE CONTENIDO

RESUMEN

El sistema utilizado por el Consejo Nacional Electoral (CNE) para escrutinios y publicación de resultados electorales presenta problemas de rendimiento, disponibilidad e integridad, según informes de la OEA y la UE. Este proyecto propone un sistema de auditoría y control electoral basado en tecnologías de registro distribuido (DLT) para mejorar estos procesos. La reforma del Código de la Democracia del Ecuador en 2020 establece un marco legal para garantizar transparencia en los procesos electorales, con disposiciones que exigen la implementación de sistemas de interconexión de datos y auditorías informáticas.

El proyecto diseñado aborda la problemática mediante el diseño de un sistema compuesto por tres componentes principales: infraestructura y seguridad, almacenamiento y redundancia de datos, y aplicación y contratos inteligentes usando blockchain. La infraestructura se basa en la tecnología PKI, el almacenamiento se gestiona mediante un sistema de archivos descentralizado, y la aplicación utiliza Hyperledger Fabric para implementar contratos inteligentes y garantizar la integridad de los datos electorales. La metodología utilizada para desarrollar el sistema está basada en análisis, diseño y prototipado, conforme a estándares internacionales y requerimientos legales del Código de la Democracia del Ecuador.

PALABRAS CLAVE: Auditoría informática, Blockchain, Transparencia electoral, Hyperledger Fabric, DLT

ABSTRACT

The system used by the National Electoral Council (CNE) for vote counting and publishing electoral results has shown performance, availability, and integrity issues, according to reports from the OAS and the EU. This project proposes an electoral audit and control system based on distributed ledger technologies (DLT) to enhance these processes. The 2020 reform of Ecuador's Democracy Code establishes a legal framework to ensure transparency in electoral processes, requiring the implementation of data interconnection systems and IT audits.

The project addresses these challenges by designing a system comprising three main components: infrastructure and security, data storage and redundancy, and application and smart contracts using blockchain. The infrastructure is based on PKI technology, storage is managed with a decentralized file system, and the application uses Hyperledger Fabric to implement smart contracts and ensure the integrity of electoral data. The methodology used to develop the system is based on analysis, design, and prototyping, in accordance with international standards and the legal requirements of Ecuador's Democracy Code.

Keywords: Electoral audit, Blockchain, Electoral transparency, Hyperledger Fabric, DLT

1 INTRODUCCIÓN

El sistema que utiliza el Consejo Nacional Electoral (CNE) para los escrutinios y publicación de resultados electorales no es confiable. Dicho sistema ha experimentado serios problemas de rendimiento, disponibilidad e integridad de la información electoral. Las misiones de observación electoral de la Organización de los Estados Americanos (OEA) y la Unión Europea (UE) han resaltado los mencionados problemas en los respectivos informes.

En el presente Trabajo de Integración Curricular (TIC) se diseñará un sistema de auditoría y control electoral para los procesos de escrutinios y publicación de resultados que lleva a cabo el CNE. Dicho sistema estará basado en tecnologías de registro distribuido (DLT, por su sigla en inglés).

La Ley Orgánica Electoral y de Organizaciones Políticas de la Republica del Ecuador o también conocido como Código de la Democracia del Ecuador en su reforma del año 2020, establece un marco legal para garantizar legalidad, equidad y transparencia dentro de los procesos electorales del país. Dentro de este marco legal, se encuentran disposiciones transitorias para definir medidas específicas que deben ser implementadas por el CNE, de tal forma que se fortalezca y modernice el sistema electoral.

La primera disposición transitoria menciona que, de forma obligatoria, el CNE, Superintendencia de bancos y Compañías de control del Gobierno Central en un plazo no mayor a 3 años, deberán implementar un sistema de interconexión de datos [1]. Dicho sistema de interconexión de datos tiene como objetivo el control del financiamiento electoral. Adicional, la sexta disposición transitoria establece que el CNE, en un plazo de 180 días deberá realizar una auditoría a su sistema informático para conteo de votos y resultados. Dicha auditoria deberá ser avalada por un organismo internacional reconocido y sus resultados deberá ser publicado en la página web del CNE [2].

El tiempo establecido para la ejecución de ambas disposiciones transitorias ha culminado y hoy en día ambos sistemas se encuentran separados y con funcionamientos distintos. Sea el caso del sistema del sistema informático utilizado por el CNE, el cual, en las elecciones seccionales del año 2023, utilizó tecnología blockchain como parte del proceso de escrutinio de actas electorales [3]. La implementación fue dada por la empresa chilena Zeyo, la cual en sus declaraciones menciona que, una vez digitalizadas las actas, cualquier persona podrá acceder a su información y verificar en tiempo real la autenticidad de un acta, garantizando autenticidad y transparencia en el proceso de escrutinio y conteo de votos [4].

La implementación de estos dos sistemas ha enfrentado varios desafíos que hoy en día hacen que el control no sea centralizado. Uno de los problemas identificados es la falta de integración de más entidades de control dentro del sistema de escrutinio del CNE. La necesidad de mejorar la trazabilidad e inmutabilidad de los datos electorales hace que necesariamente se deba distribuir el manejo y almacenamiento de los datos, así como su procesamiento y todas las acciones que se realicen en torno a documentos electorales como lo son las actas de resultados.

En el presente proyecto se propone abordad esta problemática mediante el diseño y prototipo de un sistema de auditoría y control electoral para los procesos de escrutinios y publicación de resultados. Este sistema está conformado por tres componentes principales infraestructura y seguridad, almacenamiento y redundancia de datos, y aplicación y contratos inteligentes usando cadena de bloques. A pesar de que cada componente es desarrollado de forma independiente, el prototipo junta las tres partes y funciona como un sistema único.

El enfoque de cada componente lo podemos entender de la siguiente forma:

1. Infraestructura y seguridad: En este componente se aborda el análisis, diseño y prototipo de la infraestructura y sus componentes de seguridad dados por la infraestructura de llave pública PKI, por sus siglas en inglés.
2. Almacenamiento y redundancia de datos: En este componente se aborda el análisis, diseño y prototipo del sistema de archivos descentralizado para el almacenamiento descentralizado de documentos electorales.
3. Aplicación y contratos inteligentes: En este componente se aborda el análisis, diseño e implementación del sistema de cadena de bloques, las funcionalidades de los contratos inteligentes, así como la aplicación que interactúa con la red de cadena de bloques.

En el presente documento exploraremos a detalle cada aspecto que conforma el componente de aplicación y contratos inteligentes. Se revisará el estado actual del sistema electoral utilizado por el CNE, los requerimientos existentes para la implementación del sistema descentralizado de auditoría y control electoral para los procesos de escrutinios y publicación de resultados. Luego, la metodología usada para el desarrollo del proyecto y los resultados obtenidos en base a los objetivos y alcance del proyecto.

El presente proyecto y componente fue conformado utilizando una metodología basada en las fases de análisis, diseño e implementación del prototipo. En la fase de análisis

obtenemos requerimientos tanto funcionales como legales, los cuales permitan conocer la línea base para el diseño y prototipo. Las fuentes principales para el análisis de requerimientos funcionales es la norma internacional ISO/TS 17582:2014(es) [5]. Los requerimientos legales están sustentados en el Código de la Democracia del Ecuador [1].

En base a los requerimientos funcionales y legales, en la fase de diseño plantea una propuesta para el desarrollo de un sistema de cadena de bloques que utilice tecnologías DLT, en específico la tecnología de Hyperledger Fabric, así como el uso de lenguajes de programación *Non-Turing complete* para la implementación de los contratos inteligentes.

Una vez completo el diseño, podemos desarrollar los contratos inteligentes y la aplicación cliente que se conecta con la red de cadena de bloques dada por Hyperledger Fabric. La infraestructura utilizada está basada en la red de pruebas de *Hyperledger Fabric*, *Fabric Samples* [6].

1.1 Descripción del Componente Desarrollado

En el presente componente, se diseñará los contratos inteligentes que normaran la lógica del registro de los documentos electorales y el compromiso de los integrantes que conforman la red de cadena de bloques. La estructura para conformar el proceso de registro de dispositivos emisores de actas, procesamiento y almacenamiento de actas, así como el registro de resultados. Esta estructura se traduce en el desarrollo de tres contratos inteligentes. El motivo de utilizar tres contratos inteligentes se sustenta en la necesidad de contar con un registro único para cada uno de estos tipos de información. De tal forma que se pueda consultar independientemente la información alojada en cada registro respectivo a cada contrato inteligente o *Smart Contract* por su término en inglés.

- Smart Contract de identidad: Este contrato inteligente se encarga de registrar la identidad de los computadores que actúen como controlador del scanner que digitaliza las actas de resultados electorales, el cual a su vez se lo considerará como emisor de actas, ya que es la fuente de las actas electorales digitalizadas.

  Definimos como identidad del computador la combinación de dirección IP y dirección MAC del dispositivo. Almacenar esta información entre los miembros de la red de la cadena de bloques garantiza que, es conocido los dispositivos autorizados a emitir actas.

- *Smart Contract de actas*: Este contrato inteligente se encarga de registrar las actas electorales emitidas por un computador scanner. Almacenar estas actas dentro de la cadena de bloques garantiza trazabilidad e inmutabilidad de las actas, ya que desde su creación digital se conoce las acciones que se realicen con esta, tal como modificar o eliminarla.

- *Smart Contract de resultados*: Este contrato inteligente se encarga de registrar los resultados y sumar los valores de cada acta de resultados acta ingresada a la red de cadena de bloques. Registrar los resultados en la red de cadena de bloques permite tener trazabilidad en torno a cada valor sumado en el resultado final de las elecciones electorales.

Para explorar los resultados del presente proyecto y componente, implementamos un prototipo que integra y demuestra la solución de las problemáticas descritas en la introducción. El prototipo funciona como prueba de concepto de las capacidades generales del sistema desarrollado, garantizando que los requisitos tanto legales como funcionales sean cumplidos y forme parte del proceso electoral.

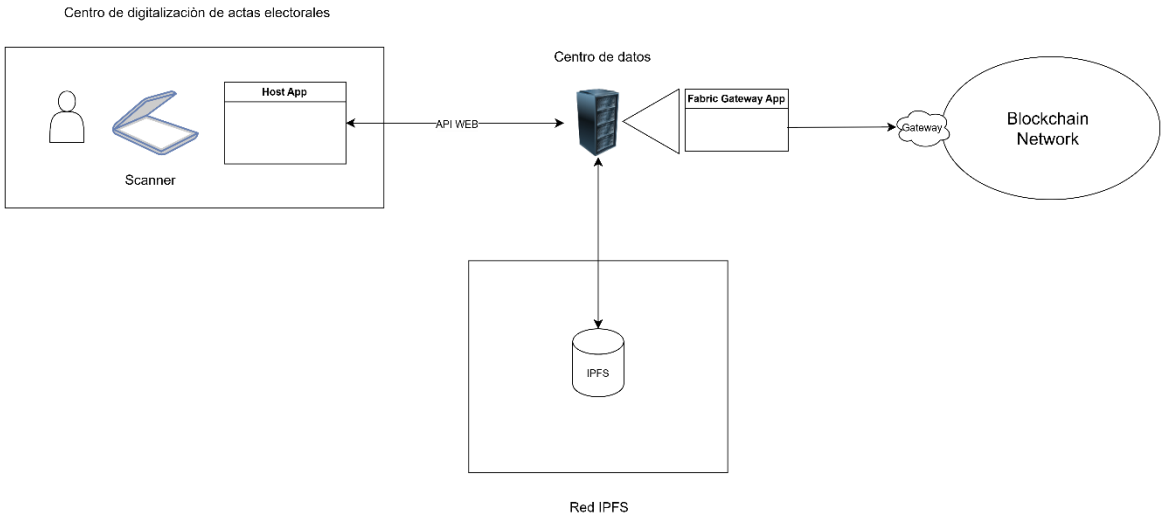


Ilustración 1.1. Esquema general de conexión

La aplicación encargada de interactuar con la red de cadena de bloques de *Hyperledger Fabric*, no simula una aplicación cliente a la cual un ciudadano pueda ingresar. Al contrario, dada las configuraciones y conexiones internas que la aplicación contiene, esta simula ser una aplicación de servidor que sirve como centro de concentración de conexiones, un nodo central al cual solo tiene accesos administradores de la red de cadena de bloques. Los

usuarios como ciudadanos o inclusive la información enviada por los computadores scanner debe ser limitada y orientada a leer o enviar información.

1.2 Objetivo general

El objetivo de este proyecto es diseñar un sistema que garantice la integridad e inmutabilidad de las actas de escrutinio digitalizadas y de los resultados electorales.

Este sistema busca asegurar que los datos almacenados sean confiables y que cualquier intento de alteración sea fácilmente detectable, proporcionando así una base sólida para la transparencia y confianza en los procesos electorales.

Para alcanzar este objetivo, se llevará a cabo un proceso detallado de diseño, análisis e implementación de un prototipo del sistema. Este prototipo servirá como una prueba de concepto que demostrará la capacidad del sistema para mantener la integridad y la inmutabilidad de los datos almacenados, así como la fiabilidad de las transacciones y los resultados obtenidos. El análisis exhaustivo permitirá identificar posibles mejoras y asegurar que el sistema cumpla con los más altos estándares de seguridad y eficiencia.

1.3 Objetivos Específicos

Analizar el sistema de escrutinios y publicación de resultados que utiliza el CNE

Este análisis busca comprender en detalle cómo opera el sistema actual y evaluar su eficiencia y efectividad en la gestión y difusión de los resultados electorales.

Para alcanzar este objetivo, se llevará a cabo un estudio minucioso del sistema actual, identificando las falencias y áreas de mejora. Este análisis permitirá detectar posibles debilidades en la infraestructura y los procesos del CNE, proporcionando información valiosa para desarrollar soluciones que fortalezcan la integridad, trazabilidad y la transparencia del sistema electoral.

Analizar los requerimientos funcionales y legales del proceso de escrutinios y publicación de resultados

Este análisis se centrará en identificar las necesidades y obligaciones que aseguren la efectividad y legalidad del sistema electoral.

Para alcanzar este objetivo, se realizará un estudio detallado de los requerimientos necesarios para garantizar la inmutabilidad, trazabilidad y consistencia de los datos. Este

análisis considerará tanto los aspectos técnicos como los legales, los cuales están establecidos por el Código de la Democracia. De esta manera, se busca asegurar que el sistema cumpla con todas las normativas vigentes y pueda mantener altos estándares de seguridad y transparencia en el manejo de la información electoral.

Diseñar la infraestructura tecnológica del sistema de cadena de bloques para el registro de las actas de escrutinio y resultados electorales

Este diseño se centrará en crear una arquitectura segura que permita almacenar y gestionar los datos electorales de manera eficiente y confiable.

Para alcanzar este objetivo, se desarrollará una aplicación cliente que permitirá interactuar con el contrato inteligente y la cadena de bloques. Esta aplicación será diseñada para facilitar el acceso y la gestión de los datos, asegurando una experiencia de usuario intuitiva y segura. El diseño incluirá todas las funcionalidades necesarias para que los usuarios puedan registrar, consultar y verificar las actas y resultados electorales, garantizando así la integridad y la transparencia del proceso electoral.

Diseñar los contratos inteligentes y la aplicación para registrar las transacciones relacionadas al proceso de escrutinios y publicación de resultados

Este diseño tiene como finalidad asegurar que todas las transacciones del proceso electoral sean registradas de manera precisa, segura y transparente.

Para alcanzar este objetivo, se desarrollarán contratos inteligentes que satisfagan las necesidades de identidad, integridad de datos y control de resultados. Estos contratos inteligentes serán diseñados para gestionar de manera eficiente la identidad de los participantes, asegurar la integridad de los datos y garantizar el control y la verificación de los resultados electorales. La aplicación desarrollada permitirá interactuar con estos contratos inteligentes, facilitando la gestión de las transacciones y asegurando que el proceso de escrutinios y publicación de resultados sea confiable y transparente.

Desarrollar el prototipo del sistema de cadena de bloques

desarrollo se centrará en crear una versión inicial y funcional del sistema que permita evaluar y validar su diseño y operatividad en un entorno controlado.

Para alcanzar este objetivo, se integrarán los tres contratos inteligentes y las tres aplicaciones respectivas en un solo sistema integrado y funcional. Esta integración asegurará que todas las partes del sistema trabajen de manera cohesiva, permitiendo una

gestión segura de las transacciones relacionadas con el proceso de escrutinios y la publicación de resultados. El prototipo desarrollado servirá como una base sólida para futuras mejoras y escalabilidad, demostrando la viabilidad y efectividad del sistema de cadena de bloques en un contexto electoral.

1.4 Alcance

El presente trabajo de integración curricular se limita en los aspectos descritos a continuación:

1. Analizar la normativa relacionada al proceso de escrutinios y publicación de resultados: La información obtenida respecto a normativas y procesos de escrutinios se limita a únicamente a la dispuesta por autoridades en internet. Otro tipo de fuentes será usado a disponibilidad. Los documentos para analizar tendrán una vigencia máxima de 10 años atrás, a partir del año 2024. El análisis realizado en base a la información obtenida se utilizará para la recolección de requerimientos, sea este funcionales o legales. El

2. Analizar el sistema que utiliza el CNE para el proceso de escrutinios y publicación de resultado: El sistema objeto a ser analizado se remite la implementación del año 2023 en donde se incorporó *blockchain* por parte de la empresa Zeyo. El material obtenido se limita al dispuesto en internet y conferencias brindadas por la empresa.

3. Diseñar la infraestructura del sistema de cadena de bloques para el registro de actas de escrutinios y publicación de resultados: La infraestructura de cadena de bloques se limita al uso de la red de pruebas de Hyperledger Fabric dispuesta en *Fabric Samples.* El proceso de registro de actas de escrutinios y publicación de resultados se traduce al diseño de dos contratos inteligentes junto con el procesamiento necesario para almacenar los datos en el registro distribuido de la red de cadena de bloques.

4. Diseñar un contrato inteligente para establecer transacciones dentro de la infraestructura de cadena de bloques: El contrato inteligente diseñado para establecer transacciones se limita a uno genérico, en el desarrollo del prototipo se especifica los tres contratos inteligentes y su funcionamiento.

5. Desarrollar un prototipo de un sistema de cadena de bloques, el cual garantice trazabilidad e inmutabilidad de los registros almacenados en la cadena de bloques: El prototipo busca realizar pruebas de concepto sobre tres ámbitos: Registrar un dispositivo emisor de actas digitales electoras dentro de la cadena de bloques, registrar un acta enviada por un el dispositivo emisor de actas dentro de la cadena de bloques, procesar y registrar los valores dentro de un acta para registrar en una cadena de bloques. El prototipo no busca estar optimizado para ejecuciones y pruebas de carga en ambientes de producción. El prototipo no busca implementar validación de valores dentro de un acta, se trabaja bajo supuestos verdaderos de los valores. El prototipo no pretende emular un ambiente de producción

1.5 Marco teórico

En la presente subsección se explicará las bases y sustento teórico para el desarrollo del proyecto de integración curricular. Las secciones para explorar son: Sistemas distribuidos, Web 3.0, sistemas DLT, contratos inteligentes, Hyperledger Fabric y Algoritmos de consenso.

Sistemas Distribuidos

Un sistema distribuido consiste en varias computadoras autónomas que se comunican y colaboran para logar un objetivo en común. Las características distintivas de este tipo de sistemas es la concurrencia de los componentes, la ausencia de un reloj global y la capacidad de operar incluso si algún componente falla. [7] Un sistema distribuido si bien, en si es una arquitectura, esta puede estar conformada de distintas formas, lo cual conlleva a diferentes subtipos, los cuales están destinadas a solventar diferentes problemas puntuales. En específico, la arquitectura utilizada en las redes de blockchain se basa en *peer-to-peer* (P2P, por sus siglas en inglés) [8].

Un sistema distribuido se constituye de varios componentes, algunos de los más importantes se detallan a continuación.

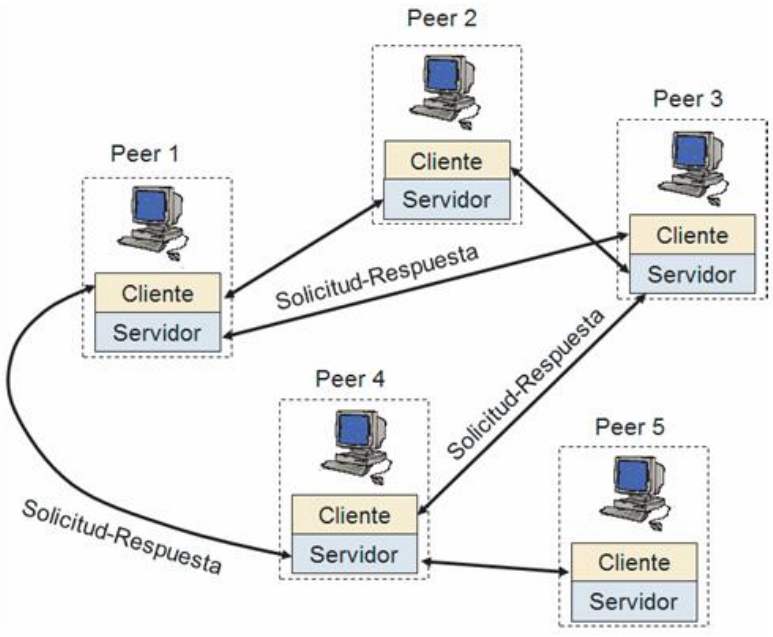


Ilustración1.5.1. Paradigma peer-to-peer [9]

Nodos

Una computadora que forma parte de un sistema distribuido se define como nodo, la cual aporta poder computacional para resolver una función en común definida dentro del sistema distribuido [10]. Si bien un nodo es una computadora, cabe recalcar que una computadora, existen varios dispositivos que son catalogados como computador, sea un servidor, computador personal o inclusive dispositivos móviles como *smartphones.* [10]

RED

El medio de comunicación por donde se distribuye la información dentro del sistema es en si el canal de comunicación. Dado que puede existir niveles de implementación de distribución la red de comunicación estar basada en redes de área local (LAN), extenderse a redes de área amplia (WAN) o lo que es usado hoy en día en sistemas ampliamente distribuidos, el internet. [10]

Middleware

Para que el sistema distribuido pueda comunicarse dentro del medio de comunicación debe existir una capa que sirva de intermediario entre la aplicación distribuida y el sistema operativo del nodo. A esta capa la denominamos Middleware, la cual dentro del modelo OSI se encuentra situada entre la capa de aplicación y la capa de transporte, tal como se detalla en la siguiente ilustración:

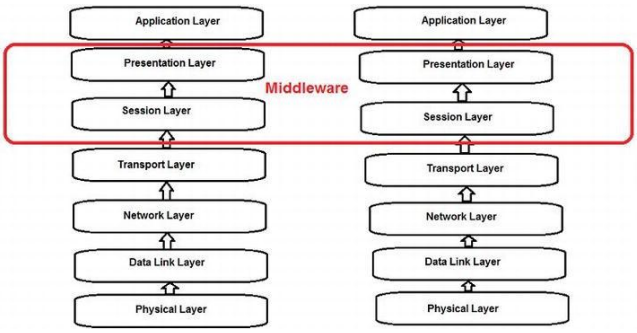


Ilustración 1.5.2. Middleware en el stack OSI [11]

El middleware establece los mecanismos para que la información heterogénea distribuida en el canal sea legible e interpretada en el nodo [8]. Los mecanismos y los atributos tratados por el middleware puede constituir una arquitectura, de la cual llamada a procedimientos remotos (*Remote Procedure Call ,* RPC, por sus siglas en inglés) es una de ellas.

- **Llamada de procedimiento remoto (RPC)**

  Las rutinas o procesos ejecutados en un computador se definen como la unidad de trabajo en un sistema computacional. Los procesos cuentan con un espacio de

memoria asignado, dicho espacio delimita los recursos, información y funciones que va a ejecutar. Cada proceso tiene independencia y no puede acceder a los elementos asignados dentro de otro proceso [12].

RPC se concibe bajo la necesidad de comunicar procesos, no en el ámbito local, ya que previamente se había implementado IPC (*inter-process communication,* por sus siglas en inglés). Si no, entre computadores remotos, dando la capacidad de ejecutar procesos remotos como si fuesen locales, bajo un esquema de cliente-servidor [12].

Una de las implementaciones de código abierto es gRPC, la cual está destinada a ejecutarse en cualquier ambiente indiferente de la heterogeneidad que pueda darse dentro del esquema cliente-servidor.

La serialización de datos es uno de los ejes centrales dentro de la comunicación dentro de los procedimientos remotos y sistemas distribuidos. Serializar datos refiere al proceso de transformar el formato de una estructura de datos en otro, el cual permita almacenar o transmitir y posteriormente reconstruir el formato y estructura de datos original [12]. Existen varias implementaciones de mecanismos de serialización, algunos de los más comunes son: JSON, XML y *Protocol Buffers*.

gRPC utiliza *Protocol Buffers (Protobuf)* como mecanismo de serialización. A diferencia de JSON, Protobuf no transforma los datos en texto plato, el formato usado por Protobuf es binario. Transformar en binario las estructuras de datos antes de ser transportadas por la red refiere una ventaja significativa en el ámbito de comunicación, una de ellas es un menor tiempo de serialización y deserialización ya que el procesamiento de etiquetas es nulo [13].

Los sistemas distribuidos pueden ser aplicados ampliamente en diferentes ámbitos, sea este para procesamiento, almacenamiento y comunicación. Una de las aplicaciones para almacenamiento de datos es *InterPlanetary File System (IPFS,* por sus siglas en inglés*).* IPFS ofrece capacidades de almacenamiento distribuido, brindando soporte para el versionamiento e inmutabilidad de datos. Los archivos añadidos a IPFS son divididos en bloques de igual longitud, los cuales se distribuyen y obtiene su hash (el cual representa su identificado). Al contar con el hash de una parte se puede juntar todos lo hashes respectivos a un archivo y obtener un nuevo hash, el cual represente el archivo, este hash es inmutable y representa la integridad del archivo [14].

Necesidad de los algoritmos de consenso

Los algoritmos de consenso son esenciales para el diseño y operación de sistemas distribuidos. A continuación, revisaremos los aspectos más críticos de la necesidad de estos algoritmos

- **Coherencia de Datos**

  Al estar los datos replicados en varios nodos. Los algoritmos de consenso aseguran acuerden el mismo estado de los datos replicados, es decir, que todos los participantes del sistema distribuido tengan los mismos datos. Esto es esencial para mantener la coherencia y prevenir inconsistencias. [7]

- **Coordinación y Sincronización**

  Los algoritmos de consenso permiten a los nodos acordar el orden de las operaciones, lo cual es crucial en sistemas de control distribuido y redes de computadoras. [7]

- **Tolerancia a Fallos**

  Los algoritmos de consenso garantizan que el sistema continue operando correctamente incluso ante del fallo de alguno de los componentes del sistema. [7] La funcionalidad es garantizada al contar con más nodos los cuales puedan efectuar el consenso. No obstante, la cantidad de nodos los cuales se encuentren disponibles para efectuar el acuerdo puede ser una limitante y causa de un fallo total, ya que se debe garantizar que al menos el 51% de nodos esté disponible, caso contrario el algoritmo no garantiza un acuerdo confiable.

- **Consistencia en la toma de decisiones**

  En muchos sistemas distribuidos es esencial que todas las copias de los datos coincidan en cada operación de actualización. Para ello, los algoritmos de consenso aseguran que, pese a fallos o problemas de comunicación, las decisiones de las operaciones sean consistentes y confiables. [7]

- **Ausencia de conflictos**

  Los algoritmos de consenso fueron ideados con el fin de evitar conflictos cuando dos o más partes deben llegar a un acuerdo. Por ejemplo, en el contexto de criptomonedas o cadenas de bloques, estos algoritmos son usados para evitar fraude y asegurar que todas las transacciones sean verificadas y aceptadas. [7]

Generales Bizantinos

El problema de los generales bizantinos es un desafío clave en sistemas distribuidos. Este dilema describe una situación en la que un grupo de generales bizantinos, cada uno a cargo de una división del ejército, debe tomar una decisión conjunta en si atacar o retirarse. El problema radica en la existencia de un traidor entre los generales, el cual pueda enviar mensajes engañosos a los demás. [15]

El desafío de los generales bizantinos radica en la necesidad de que los generales lleguen a un consenso, asegurando que todos tomen una decisión conjunta mayoritaria y favorable para todo el ejército, a pesar de la presencia de generales traidores y de las limitaciones de la comunicación entre ellos. [15]

El enfoque del problema de los generales bizantinos es resolver un problema de confianza. Dentro del problema se establecen directrices para poder llegar a una solución:

- Todos los generales deben estar comunicados entre si y deben decidir una acción a la vez.
- Si todos los generales, o su mayoría, están de acuerdo en una decisión, todos los generales deben acordar ejecutar esa decisión.

La resolución de este problema radica en la comunicación y que la base de confianza está en la mayoría de los votos. [16]

Varios de los algoritmos de consenso tratan el tema de la confianza desde diferentes acercamientos, no obstante, el uso de estos algoritmos puede repercutir impactos ambientales dada su naturaleza de cómputo. Dentro de la red Blockchain de Bitcoin se implementa el algoritmo de consenso por prueba de trabajo (*Proof of Work, PoW* por sus siglas en inglés). PoW está enfocado en calculo por fuerza bruta para encontrar un hash valido capaz de cumplir una condición base determinada por la cantidad de miembros en la red blockchain de bitcoin. En el 2024, Digieconomist sitúa en el puesto 25 el consumo de Bitcoin si fuese un país, estado por encima de países como Malasia y debajo de Polonia [17].

El uso de algoritmos basados en la capacidad de cómputo, si bien pueden ser beneficiosos en un ambiente de confianza cero, son totalmente inadecuados en un entorno permisionado y privado, donde todos sus miembros son autenticados. Es allí donde el uso de algoritmos de consenso como *Byzantine Fault Tolerance* (BFT, por sus siglas en inglés) sea usado, ya que el consenso no radica en pruebas de fuerza de cómputo, si no en consenso lógico y basado en la confianza.

Sistemas Centralizados

En un sistema centralizado la toma de decisiones y el control operativo están centrados en una única entidad o autoridad central. Este tipo de estructura implica que las funciones clave, las decisiones estratégicas y la administración son gestionadas desde un punto centralizado de autoridad. [18]

Sistemas Descentralizados

Un sistema descentralizado distribuye el control y la toma de decisiones entre múltiples entidades o nodos. En este tipo de sistemas no hay una autoridad central que controle las decisiones, en su lugar, las decisiones pueden ser tomadas por varios nodos de manera colaborativa o independiente. [18]

Web 3.0

La web 3.0 hace referencia a la revolución del internet como una plataforma descentralizada, en la que sus usuarios tengan mayor control sobre sus datos y transacciones. [18]

Problemas Web 2.0

- Los sistemas Web 2.0 están dominados por plataformas centralizadas que controlan gran parte de la información e interacciones en línea.
- Los sistemas enfrentan problemas de privacidad debido a la recopilación masiva de los datos y la falta de control por parte de los usuarios sobre su información personal.
- La centralización conlleva riesgos de seguridad, exponiendo los sistemas a posibles ataques. [18]

Soluciones Web 3.0

- En la web 3.0, utilizando tecnologías como Blockchain, descentraliza la estructura y permite a los usuarios tener más control sobre sus datos e interacciones.

- Ofrece un mayor control a los usuarios sobre quien puede acceder a sus datos y como se utilizan.
- Promueve la transparencia para mantener un registro público y verificable de las transacciones, lo que disminuye la posibilidad de manipulación o fraude. [18]

Estado del arte en la Web 3.0

Blockchain y criptomonedas

La web 3.0 se distingue en la descentralización y en el uso de tecnologías como blockchain y criptomonedas, como Bitcoin. Estas tecnologías permiten realizar transacciones peer-to-peer sin la necesidad de un intermediario. [19]

Descentralización

Promueve el desarrollo de aplicaciones descentralizadas. Estas aplicaciones operan sobre blockchain y otros sistemas descentralizados, lo que los permite funcionar de manera autónoma. [19]

Identidad digital y privacidad

La web 3.0 tiene como objetivo dar la capacidad a los usuarios de gobernar las acciones que se realizan sobre sus datos personales. [19] Dentro de la web 3.0 la identidad es un elemento importante y centrada en el usuario. Los usuarios tienen control total de su identidad y son dueños de las decisiones y lugares en donde compartir esta información.

Dada la naturaleza descentralizada de la web 3.0, mantener la privacidad e identidad de los usuarios es sumamente valioso al integrarse capacidades de trazabilidad de transacciones y seguimiento de información. Esto permite a organizaciones, usuarios y sitios de internet ser transparentes con la información que almacenan, manipulan y transfieren.

Varios de los desafíos de la web 3.0 radican en la adopción de las nuevas tecnologías y normas legales, ya que mucha de la información almacenada actualmente en la web 2.0 está gobernada por legislaciones locales de cada país. Dentro de internet existen pocas legislaciones estándar para el manejo y control de la información, no obstante, la adopción de estas normas es subjetiva de cada país.

Interoperabilidad

Mejorar la interoperabilidad entre diferentes blockchains y sistemas descentralizados, estableciendo estándares y protocolos para que estos sistemas se puedan comunicar de manera eficiente y segura. [19]

Distributed Ledger Technology (DLT)

Tecnología de Libro Mayor Distribuido (DLT, por sus siglas en inglés), es una tecnología que permite e a múltiples participantes mantener y actualizar de manera sincronizada y consensuada un registro compartido a través de una red descentralizada. A diferencia de un sistema centralizado que depende de un único repositorio, DLT distribuye copias idénticas del registro a todos los nodos de la red. Cada nodo posee una copia del libro mayor, y todas las actualizaciones se distribuyen a través de la red utilizando algoritmos de consenso, lo que garantiza que todos los participantes compartan una visión unificada de la información en tiempo real. [20]

Trazabilidad

La trazabilidad dentro de una red blockchain refiere a la capacidad de rastrear el historial completo de las transacciones. Cada una de estas transacciones, dentro de una red blockchain, se registran de manera secuencial en bloques que están conectados mediante criptografía. La trazabilidad es crucial para garantizar la transparencia, la inmutabilidad y la capacidad de auditar registros. [20]

Integridad

La integridad dentro de la cadena de bloques (blockchain) se logra mediante el uso de funciones hash criptográficas y el consenso distribuido. Cada bloque en la cadena contiene un hash del bloque anterior, creando una cadena continua e ininterrumpida. Cualquier intento de modificar los datos en un bloque previo cambiaría su hash, lo que sería detectado de inmediato por la red descentralizada, garantizando así la integridad de la información [20].

Cadena de bloques

Cadena de bloques o blockchain, es una estructura de datos lineal y secuencial, compuesta de bloques los cuales se encuentran interconectados. Cada bloque contiene un grupo de transacciones verificadas y un hash que enlaza al bloque anterior, formando una cadena continua desde el primer bloque (conocido como el bloque génesis) hasta el bloque más reciente. [20]

Tipos de cadena de bloques

Públicas

Las cadenas de bloques públicas, como Bitcoin y Ethereum, permiten el acceso a cualquier persona interesada en participar en la red, descargar el ledger (Libro mayor distribuido) y validar transacciones. La seguridad de esta cadena de bloques radica en el consenso distribuido y utilizar mecanismos de prueba, como Proof of Work (PoW) en el caso de Bitcoin. [20]

Permisionadas

Las cadenas de bloques permisionadas restringen el acceso y la participación a un grupo de participantes autorizados. Estas redes se utilizan principalmente en aplicaciones empresariales o gubernamentales, donde es necesario tener un mayor control sobre la confidencialidad de los datos [20].

Smart Contracts

Los contratos inteligentes o también conocidos por su término en inglés *Smart Contracts* son programas informáticos enfocados a utilizarse en una red blockchain y cuyo propósito es facilitar, verificar o hacer cumplir una negociación entre dos o más involucrados. Nick Szabo, pionero en el área de criptografía en 1997 los definió como “protocolos de transacción computarizados que ejecutan los términos de un contrato” [21].

Los contratos inteligentes funcionan a través de acuerdos y reglas específicas que permiten delimitar resultados específicos. Una característica principal de los contratos es que deben ser deterministas [22]. Ya que, los algoritmos de consenso que rigen cuando se aprueba una transacción deben evaluar resultados iguales. Por esta razón, todas las ejecuciones de un contrato inteligente con las mismas entradas deben llegar al mismo resultado [22].

Los contratos inteligentes cuentan con el avalúo de ser transparentes y generar confianza al ser distribuidos y dependientes del consenso.

Para que un contrato inteligente funcione dentro de una red de bloques, este primero debe distribuirse en todos los participantes de la red, es instalado en cada miembro, a los cuales se los denomina *peer*. El peer espera el llamado o cumplimiento de condiciones para ejecutar una rutina establecida dentro del contrato inteligente [22].

Los lenguajes utilizados para desarrollar los contratos inteligentes se dividen fundamentalmente en dos tipos:

- Lenguajes completos: Este tipo de lenguajes de programación son aquellos que pueden realizar cualquier tipo de cálculo computacionalmente posible ya que utilizan instrucciones que necesariamente no establecen resultados deterministas [23]. Un ejemplo de este tipo de lenguajes es GO.
- Lenguajes no completos: Este tipo de lenguajes son aquellos que no cumplen con todos los criterios para realizar cualquier calculo computacionalmente posible. La característica principal radica en la limitación de saltos de ejecución, lo cual quita la posibilidad de ejecutar bucles, condiciones u otro tipo de operación presente en la máquina de Turing [23]. Un ejemplo de este tipo de lenguajes en Solidity

Dada la naturaleza de los contractos inteligentes, los lenguajes no completos son usados ampliamente en implementaciones de cadenas de bloques. Tal es el caso de Bitcoin, que utiliza un lenguaje no completo. Este lenguaje está diseñado para realizar operaciones básicas necesarias en las transacciones, tales como verificar firmas o bloques de monedas [23].

A diferencia de Bitcoin, la cual es una plataforma pública y de uso de lenguajes no completos, existe otras plataformas con enfoques distintos, permisionadas y de lenguaje completo, como lo es Hyperledger.

Hyperledger Fabric

Hyperledger Fabric es una plataforma DLT, diseñada para usos empresariales. Es una plataforma de código abierto. Esta plataforma ofrece una arquitectura modular que proporciona la flexibilidad y privacidad necesarias para aplicaciones empresariales que requieren un alto grado de confidencialidad y control [6].

Características Hyperledger Fabric

- Hyperledger Fabric permite modularidad en componentes clave como el consenso, la privacidad de datos y los contratos inteligentes. El modularidad facilita la adaptación de la plataforma a una amplia variedad de requisitos empresariales específicos.

- Ofrece la capacidad de establecer canales de comunicación privados entre participantes específicos dentro de la red, garantizando que solo los usuarios autorizados tengan acceso a cierta información.
- Está diseñada para manejar un alto volumen de transacciones.
- Permite la implementación de contratos inteligentes, que son acuerdos programables entre participantes de la red que se ejecutan automáticamente bajo condiciones predefinidas.
- Proporciona opciones de consenso adaptables, permitiendo a los participantes de la red elegir el algoritmo de consenso más adecuado para sus necesidades particulares.
- Integra un sistema de gestión de identidad que permite autenticar y autorizar a los participantes de la red, además de definir políticas de acceso detalladas.
- Facilita la auditoría de transacciones mediante la capacidad de rastrear y revisar todas las actividades registradas en la red de blockchain, lo que asegura una transparencia completa. [6]

Algoritmos de Consenso

Dentro de la red de blockchain, un algoritmo de consenso es utilizado por los nodos para llegar a un acuerdo sobre el estado del sistema, o la validez de los datos alojados en la red. Los algoritmos de consenso están diseñados para asegurar que todos los nodos dentro de la red estén de acuerdo en la ejecución y validez de las transacciones. [18]

Crash Fault Tolerance (CFT)

Algoritmos utilizados para fallas no maliciosas, tales como errores de hardware, software. Estos algoritmos garantizan que, si algún nodo falla, o se envían alguna información incorrecta sin fines maliciosos, el consenso global se mantenga. [18]

Byzantine Fault Tolerance (BFT)

Algoritmos utilizados en redes donde su principal desafío es la confianza. Está diseñada para manejar comportamientos arbitrarios o malicioso. En un sistema con algoritmos BFT

implementados los nodos participantes llegan a un acuerdo incluso en la presencia de nodos maliciosos. [18]

2 METODOLOGÍA

Para el presente TIC, se utilizó tres fases base de una metodología tradicional, análisis, diseño y desarrollo de prototipo. La fase de pruebas se ha desarrollado en base a pruebas de concepto, las cuales buscan determinar la funcionalidad del prototipo desarrollado.

En la fase de análisis se revisó el estado actual del sistema de escrutinio y publicación de resultados del CNE. Este análisis permitió conocer puntos de mejora dentro del sistema, así como el cumplimiento de normas legales normas que rigen el ámbito funcional de sistemas electorales. Las fuentes de información en las cuales se basó el presente TIC fueron conferencias dictadas por el mismo CNE, documentación mostrada por Zeyo en las Jornadas JISIC 2024 impartidas por la Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional. Estas conferencias fueron de vital importancia en la recolección de información sobre el estado actual del SIER ya que la información brindada en internet es escasa.

En la fase de diseño, se definió la arquitectura, funcionalidad y cambios que deben ser implementados dentro del sistema actual del CNE, a fin de mejorar la trazabilidad y confianza dentro de los procesos electorales.

En la fase de desarrollo de prototipo, se validó el diseño mediante la implementación de funciones base, las cuales definen una prueba de concepto dentro de la funcionalidad general del sistema de escrutinio y publicación de resultados del CNE. El prototipo implementa tecnologías de sistemas distribuidos como lo es *Hyperledger Fabric* e IPFS.

2.1 Análisis

Análisis del sistema actual de escrutinios y publicación de resultados

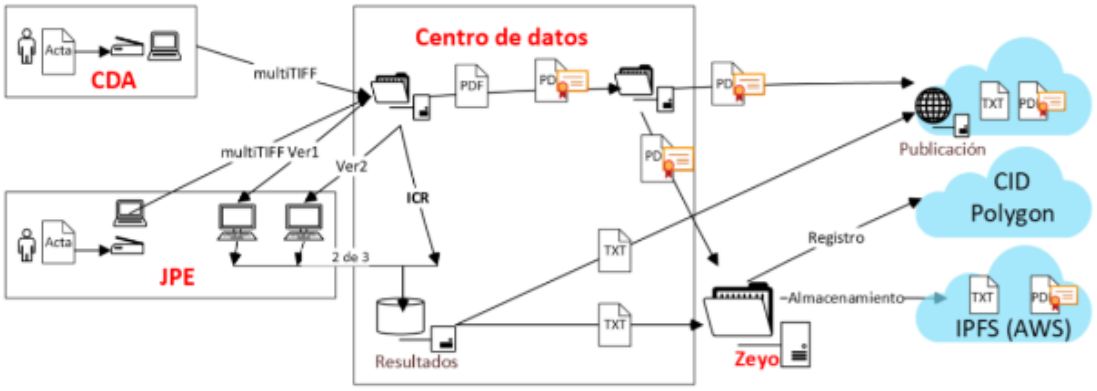


Ilustración 2.1 Arquitectura actual SIER

La ilustración 2.1 ilustra el estado actual del sistema de escrutinios y publicación de resultados del CNE, formalmente conocido como Sistema Informático de Escrutinios y Resultados (SIER), creado y desarrollado por el CNE. El SIER está conformado por módulos, de los cuales se define a continuación:

Módulo de escrutinios

El modulo de escrutinios es el responsable de recolectar, procesar y almacenar las actas dentro de la red de Polygon, el proceso es descrito a continuación:

- Las actas físicas son digitalizadas mediante scanner, los cuales están conectados a computadores, estos envían los archivos correspondientes al acta a un servidor de archivos.
- Debido a la dinámica del país, no todos los recintos cuentan con centros de digitalización de actas, razón por la cual las actas de resultados son enviadas hacia juntas provinciales electorales, las cuales digitalizan y envían esta información a los centros de procesamiento de datos del CNE.
- Las actas receptadas en el centro de datos del CNE son alojadas en el servidor de archivos, para luego ser convertidas en PDF y firmadas, posteriormente son almacenadas en una red de IPFS externa.
- Para el reconocimiento y cálculo de valores de resultados, las actas pasan por un proceso de reconocimiento de caracteres (*Intelligence character recognition*, ICR por sus siglas en inglés) en los cuales se envía secciones de las actas a juntas provinciales delegadas para la digitación de los valores escritos en actas. Este proceso se repite para varias juntas y el sistema de reconocimiento en sí. La decisión final está definida por la mayoría de las coincidencias.

- Una vez procesado los datos de un acta, estos valores pasan a formar parte de la tabla de resultados, en la cual se procesa y asigna los valores. El acta y la tabla de resultados es enviada hacia IPFS para ser almacenada. IPFS retorna identificadores de contenido para cada archivo, estos identificadores son enviados a la red de Polygon, y los archivos a un servidor en la nube.

Dentro de este esquema existen dos problemas sustanciales. El primer problema está relacionado a la trazabilidad, la implementación de blockchain no es completa y no existe trazabilidad desde la digitalización del acta hasta su posterior almacenamiento en IPFS. La manipulación del acta no es registrada y está sujeta a disposición únicamente del CNE.

El segundo problema es la centralización del registro y almacenamiento. Dentro de esta red no existe participación de otras entidades de control, lo cual disminuye la confianza y no garantiza el avaluao de las mismas. Si bien Polygon e IPFS son soluciones descentralizadas, el control y envío de la información depende exclusivamente del CNE y Zeyo.

Para poder plantear una solución acorde a los requerimientos funcionales y legales del País se requiere analizar a detalle normativas que refieren a procesos electorales, tal es el caso de El Código de la Democracia (Registro Oficial N.º 134) y La norma ISO/TS 17582:2014(es).

Código de la Democracia

Dentro del código de la democracia, en su primera disposición transitoria establece que:

“Primera.- El Consejo Nacional Electoral, Superintendencias de Bancos y Compañías y las respectivas entidades de control del Gobierno Central, deberán generar un Sistema de Interconexión de Datos en un plazo de ciento veinte días desde promulgada la presente Ley Reformatoria a la Ley Orgánica Electoral y de Organizaciones Políticas, Código de la Democracia.” [1]

Esta disposición establece la participación de entidades de control del Gobierno sobre un sistema de interconexión para el control del gasto electoral de los partidos políticos. Si bien el enfoque de esta disposición es realizar el control financiero de los partidos políticos, permite tener un acercamiento a un sistema interconectado entre figuras de control, lo cual permite tener un acercamiento hacia otros temas de interés, como lo es el control del proceso de escrutinio y publicación de resultados. De esta forma, figuras de control y regulación pueden incluirse en este sistema y realizar el seguimiento y, permitiendo aumentar la confiabilidad e integridad de los procesos electorales.

Dentro del código de la democracia, en su segunda disposición transitoria establece que:

> “Segunda.- El Consejo Nacional Electoral en un plazo de tres años, implementará el Sistema de Interconexión de Datos para control del financiamiento a la política. En adición a las instituciones dispuestas en la presente Ley Orgánica Reformatoria, el Consejo Nacional Electoral podrá añadir a aquellas otras instituciones, públicas, que estime pertinente para las atribuciones y facultades de control a su cargo.” [1]

Esta disposición establece la implementación obligatoria en un tiempo plazo de tres años a partir del 2020. En marzo del 2024 en la sesión de rendición de cuentas del año 2023. La presidenta del CNE declaró que el sistema fue implementado y existe la interconexión entre las autoridades de control mediante una rueda de prensa en el marco de rendición de cuentas del año 2023. [24]

Dentro del código de la democracia, en su sexta disposición transitoria establece que:

“Sexta.- El Consejo Nacional Electoral, tendrá un plazo de ciento ochenta días a partir de la entrada en vigencia de esta Ley, para realizar una auditoría a su sistema informático para conteo de votos y resultados. Esta auditoría debe ser avalada por un organismo internacional reconocido y sus resultados deberán publicarse en la página web del Consejo Nacional Electoral.” [1]

La auditoría solicitada a partir de esta disposición transitoria no pudo ser efectuada en el plazo dado, ya que para el año 2021 se estaban ejecutando el proceso electoral de Elecciones Generales 2021. De acuerdo con las declaraciones de la presidenta del Diana Atamaint el CNE y la Contraloría General del Estado mantienen un acuerdo institucional el cual permite postergar actividades de auditoria en el sistema electoral mientras no concluya un proceso electoral en curso [2]. La disposición explícitamente menciona que los resultados de dicha auditoria debe ser accesible desde la página web del CNE. En el mes de agosto del 2024 los resultados de esta auditoria no están accesibles, con lo cual se induce que no se está cumpliendo a cabalidad la disposición.

La auditoría solicitada a partir de esta disposición transitoria no pudo ser efectuada en el plazo dado, ya que para el año 2021 se estaban ejecutando el proceso electoral de Elecciones Generales 2021. De acuerdo con las declaraciones de la presidenta del Diana Atamaint el CNE y la Contraloría General del Estado mantienen un acuerdo institucional el cual permite postergar actividades de auditoria en el sistema electoral mientras no concluya un proceso electoral en curso [2]. La disposición explícitamente menciona que los

resultados de dicha auditoria debe ser accesible desde la página web del CNE. En el mes de agosto del 2024 los resultados de esta auditoria no están accesibles, con lo cual se induce que no se está cumpliendo a cabalidad la disposición.

Norma ISO/TS 17582:2014(es)

La norma ISO/TS 17582:2014(es) titulada “Calidad en la administración electoral “Requisitos de calidad para los organismos de administración electoral en la gestión de procesos electorales” proporciona una seria de requisitos para la gestión electoral efectiva y eficiente de parte de los organismos de administración electoral.

En el año 2016, el CNE celebró haber sido reconocidos por haber cumplido con éxito el proceso de auditoría necesarios para certificar ciertos procesos con la Especificación técnica ISO/TS 17582:2014. Alguno de los procesos que fueron certificados son: registro de votantes, organizaciones políticas, candidatos, logística electoral, votación, conteo de votos, declaración de resultados, entre otros más [25].

Para el proceso de conteo de votos, la norma ISO refiere que los registros de escrutinio de votos deberán producir registros de salida del proceso. El registro deberá incluir información como: identificador único de la estación de voto, número total de votantes, número de votantes por candidato, número de votos válidos, número de votos blancos, número de votos nulos [5].

En cuanto a la infraestructura necesaria, la norma ISO refiere que, como mínimo se deberá especificar un canal de comunicación de los resultados de las votaciones, y otras consideraciones para el área física de trabajo donde se efectúa el voto, como lo es los recintos electorales.

El proceso de escrutinio es fundamental dentro de todo el macroproceso de elección de autoridades mediante la elección de autoridades mediante el sufragio ciudadano, adicional considerar que disposiciones tales como las mencionadas en el Código de la democracia refieren a demostrar que los procesos han sido efectuados en el marco de la ley. Por estas razones, se considera que el proceso de escrutinio como el de publicación de resultados debe cumplir con la triada de seguridad de la información: Integridad de los datos, Confidencialidad de los datos y disponibilidad de los datos.

Para que los datos electorales sean íntegros, estos deben ser inmutables y dicha inmutabilidad debe ser posible de ser verificada. Una red blockchain permite mantener datos inmutables mediante la replicación de datos, de tal forma que, cualquier cambio

realizado puede ser verificado y comprobado. Si un dato electoral es alojado dentro de una red blockchain, este dato se mantendrá registrado y replicado, con lo cual cualquier cambio será registrado, dando a lugar la inmutabilidad y verificación del mismo.

Para que los datos electorales sean confidenciales, se debe establecer un nivel de acceso a la información y datos electorales. En este caso, los datos electorales deben ser de acceso público, ya que se busca la transparencia en el proceso. Para garantizar que los datos sean confidenciales, se deberá almacenarlos en repositorios de acceso libre para que la ciudadanía tenga a disposición la lectura de los datos electorales, como lo es las actas de resultados o tabla de resultados finales.

Para que los datos electorales estén disponibles, se deben replicar y disponer al publico su acceso. Dentro de un sistema distribuido, la replicación de datos permite que el acceso a la información sea más rápida y segura que un sistema convencional y centralizado, ya que la redundancia garantiza que los datos se encuentren distribuidos y accesibles en todo momento, mientras los miembros del sistema estén disponibles y accesibles.

2.2 Diseño

El diseño del sistema esta basado en la plataforma de sistemas distribuidos de cadena de bloques Hyperledger Fabric. Las componentes del modelo de *Hyperledger Fabirc* se describe a continuación:

Asset: Un Asset o activo se define como cualquier cosa que tenga un valor sobre la red de blockchain y que se desea registrar

Chaincode: Un chaincode o código de cadena es la parte lógica que rige las transacciones y que permiten manipular y modificar un Asset.

Ledger: El ledger o registro es el registro inmutable en el cual se almacena las transacciones realizadas. Este elemento puede ser consultado mediante solicitudes similares a SQL [26].

Privacidad: La privacidad dentro de la red de *Hyperledger Fabric* está definida mediante un canal de comunicación. Los miembros de un canal son los únicos capaces de poder operar con los elementos dentro de este, como lo es el ledger y los assets almacenados [26].

Seguridad y Servicios de membrecía: La membrecía dentro de la red de *Hyperledger Fabric* está garantizada y definida mediante el uso de una infraestructura de llave publica, mediante la cual se establece los certificados para las organizaciones y sus participantes.

Solo aquellos participantes verificados mediante su certificado público pueden acceder e interactuar en la red de Hyperledger Fabric [26].

Consenso: Dentro del ambiente distribuido de Hyperledger Fabric, el consenso es un elemento principal dentro de la red. Para que las transacciones realizadas dentro de la red deben existir consenso dentro de los participantes. Para el manejo del consenso de las transacciones existen algoritmos que pueden ser utilizados, tal es el caso del algoritmo BFT o RAFT [26].

Una vez entendido como se compone el modelo de Hyperledger Fabric podemos analizar la composición de la red de Hyperledger Fabric y como sus miembros se incorporan en este:

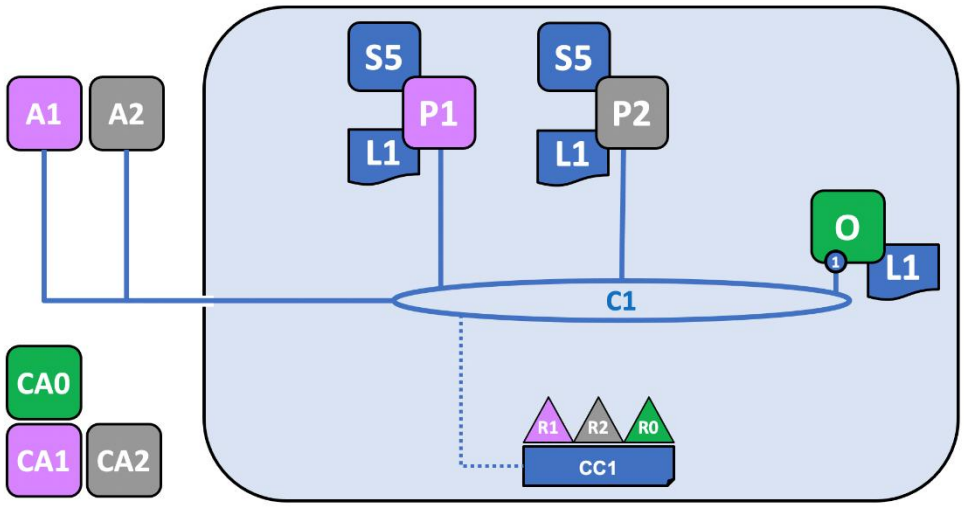


Ilustración 2.2.1 Fabric test Network [27]

En la ilustración 2.2.1 podemos observar como se encuentra organizada la red de Hyperledger Fabric en su modelo de pruebas llamada *Test-Network.* Dentro de esta red existen elementos como: Entidades certificadoras para cada organización, canal, aplicación, Organización y sus peer, Ordenador, Chaincode, y. A continuación, se detalla la información de cada elemento de la red.

Entidades certificadoras (CA)

Para que una organización forme parte de la red de Hyperledger Fabric se debe establecer un mecanismo de autenticación entre los diferentes integrantes de la red. Para este propósito Hyperledger ofrece la capacidad de incorporar una infraestructura de llave publica a la red, con lo cual cada organización debe contar con una entidad certificadora que emita material criptográfico como certificados y llaves asimétricas para cifrar y descifrar la información transmitida en la red.

La forma de que cada miembro de una organización pueda utilizar el mecanismo de autenticación es resuelto mediante una estructura llamada *Membership service provider (MSP,* por sus siglas en inglés*).* El MSP permite que un miembro de una organización utilice su certificado alojado en un directorio específico del MSP para enviarlo a otro miembro y demostrar su identidad. Dentro del mismo MSP se encuentra un directorio en donde se almacena los certificados del resto de miembros, así como de autoridades de la red. De esta forma toda interacción es verificada utilizando el material criptográfico alojado en el MSP de cada miembro.

Canal(C)

El canal es una abstracción para definir un espacio en donde se definen miembros, políticas y medios de comunicación. Dentro del canal se establece un acuerdo entre todas las organizaciones miembros para aceptar este acuerdo y establecer el canal como medio de comunicación. Dentro del canal se aloja únicamente un chaincode. Solo los miembros del canal pueden acceder al ledger y assets asociados.

Organización (O)

Una organización se define como el espacio lógico en el cual se establece una entidad la cual se organiza elementos propios para su funcionamiento dentro de Hyperledger Fabric. Dentro de la dinámica de Hyperledger Fabric, lo que se busca es interconectar organizaciones y que la interacción entre estas sea permisionada, segura y registrada. La interconexión de las organizaciones debe permitir compartir registros de actividad y que el proceso de almacenamiento y manipulación sea consensuado.

Peer (P)

Un peer se define como un miembro de una organización, definitivamente es un computador que almacena el ledger y ejecuta el chaincode definido en el canal al cual pertenece. Un peer puede pertenecer a varios canales, tantos como la organización pertenezca. Cabe aclarar que una organización puede contar con varios peers, un peer puede ser designado como representante de la organización y receptar las transacciones que se solicitan aprobar dentro de la red de Hyperledger Fabric.

Un peer almacena el ledger (L) el cual es un registro que contiene todas las transacciones realizadas en el canal. Este registro se sincroniza con cada transacción aprobada dentro del canal. Un peer puede tener varios ledgers ya que puede pertenecer a varios canales.

Un peer almacena el chaincode (S) el cual contiene las reglas y transacciones validas dentro del canal. Un chaincode puede almacenar varios contratos inteligentes, los cuales

definen diferentes enfoques y reglas de lógica, esta abstracción permite tener control y orden dentro de cada transacción y enfoque que se quiera dar. Cada transacción debe estar asociada a una función definida en un contrato inteligente dentro del chaincode.

Ordenador (O)

Un ordenador es un peer de una organización, esta organización puede ser una específicamente designada para intermediar y orquestar las transacciones, como lo puede ser un peer de una organización miembro. El objetivo del ordenador es receptar las solicitudes de una organización para registrar una transacción en el resto de las organizaciones, mediante un algoritmo de consenso, se realiza la ejecución de la misma transacción solicitada, si el resultado es el mismo y las organizaciones están de acuerdo, se procede a solicitar el registro de la transacción en todas las organizaciones miembro.

App(A)

La aplicación es un elemento de entrada a la red de Hyperledger Fabric, es la interface que permite conectarse con la red, ya que de forma individual desde cada peer no es recomendado interactuar con la red, si no de forma externa mediante una aplicación. Existe dos formas para conectarse con la red, la primera es utilizando la interface peer provista por Hyperledger, la cual mediante el paso de los elementos del MSP como parámetros, permite realizar consultas al peer y consecuentemente al ledger. Otra opción es utilizar el SDK de Hyperledger en el cual se ofrece una abstracción de la interface peer. Esta abstracción se llama Gateway App, la cual permite realizar la conexión hacia el peer una sola vez y realizar múltiples consultas solo con el nombre de las funciones de los contratos inteligentes y sus parámetros.

Una vez que conocemos los elementos de la red de Hyperledger Fabric, podemos definir el esquema y aplicación para el Sistema Informático de Escrutinios y Resultados del CNE.

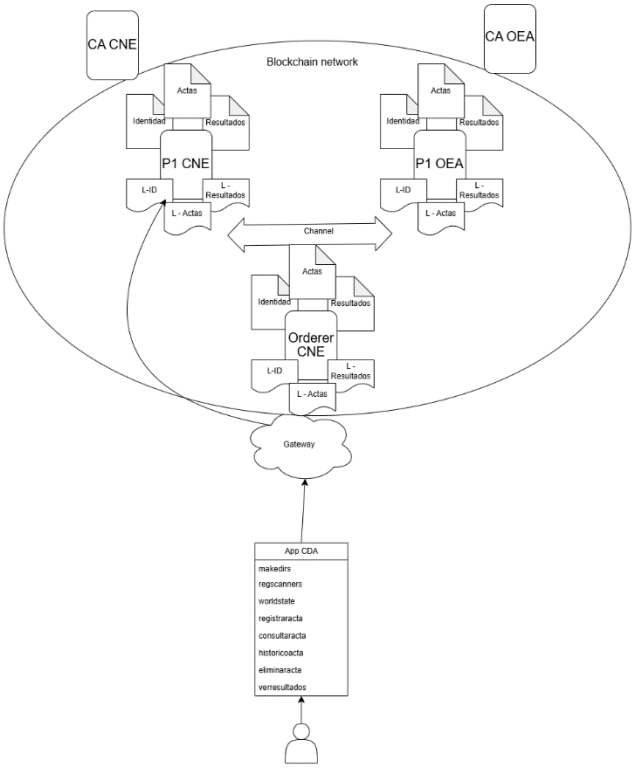


Ilustración 2.2.2 Arquitectura cne-network y App Gateway

Dentro de la ilustración 2.2.2 podemos identificar los elementos que componen la red de Hyperledger. Si tomamos como ejemplo la organización CNE, contamos con una entidad certificadora, un ordenador, un peer, el canal en el cual se comunica con la organización CNE con la organización OEA, y finalmente los ledgers y contratos inteligentes asignados.

Para poder controlar los dispositivos conectados a los scanners en los centros de digitalización de actas electorales o en las juntas provinciales, se debe listar los elementos los dispositivos que se comunicarán con la aplicación. Una opciòn para poder obtener esta informaciòn es que el CNE 3 dìas previos al día de las elecciones, mediante un acta notariada, liste los computadores que haràn uso de este scanner y seràn los encargados de digitalizar las actas electorales. De esta forma se tiene control de aquellos dispositivos que seràn los ùnicos autorizados en enviar actas al centro de procesamiento.

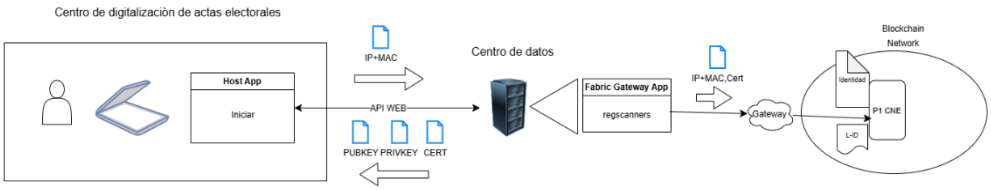


Ilustración 2.2.3 Flujo de trabajo registro de identidad

En este escenario, se conoce previamente los dispositivos que van a digitalizar actas, estos computadores tienen una app, que mediante una conexión web, envian sus datos de identificación. En un primer alcance la identificación del dispositivo es su dirección IP y su Dirección MAC de la interface de red conectada. La informaciòn es receptada en el centro de procesamiento, en donde se genera el material criptográfico para el dispositivo (certificado digital y llaves asimétricas) haciando uso de la entidad certificadora del CNE.

Una vez obtenido el material criptográfico basado en la identididad del dispositivo, estos datos se registrá en la red de Hyperledger. Los datos de identificacion permanecerán inmutables en los registros de cada peer de la red de Hyperledger, lo cual da constancia de los dispositivos autorizados. El material criptográfico es entregado al computador digitalizador para que pueda firmar las acta electorales.

Una vez que se ha registrado el dispositivo se podrá realizar el proceso de escrutinio y publicación de resultados.

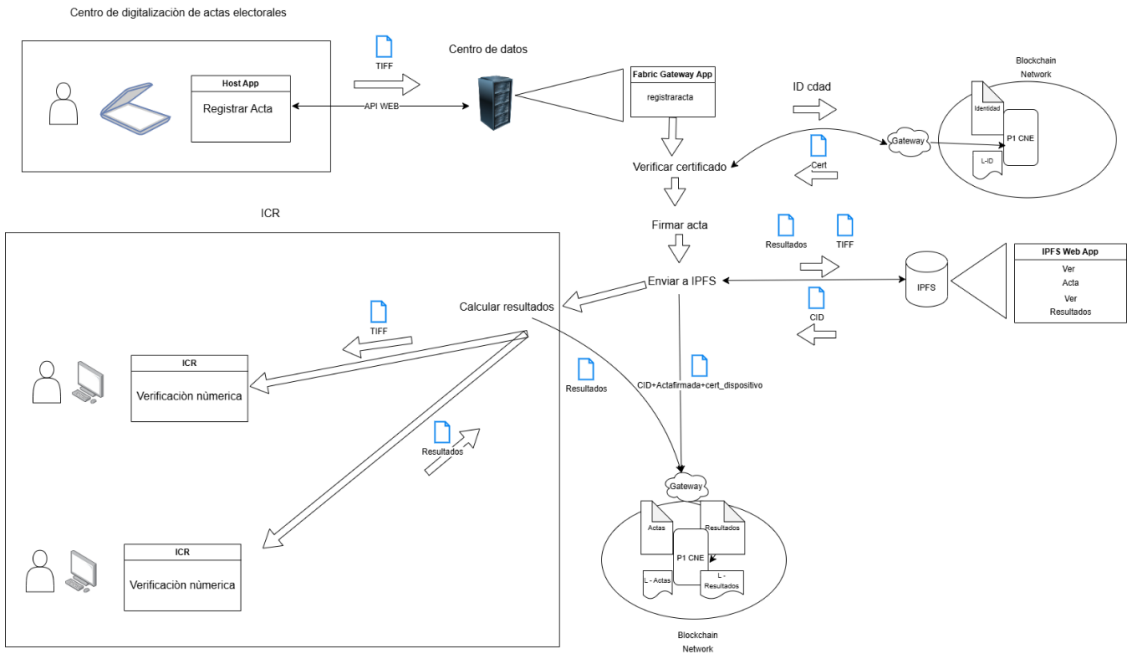


Ilustración 2.2.4 Flujo de trabajo registro de acta

En la ilustración 2.2.4 se puede apreciar el funcionamiento símil al implementado actualmente por el CNE, ciertos elementos fueron eliminados, ya que no representan un aporte efectivo en el proceso.

Los computadores que digitalizan actas, los denominaremos cdad. Un cdad cada vez que digitaliza un acta, envía el documento firmado hacia el centro de datos del CNE. Dentro del centro de datos, se procesa la información respecto al acta realizando una consulta a al ledger de identidad dentro de la red de blockchain. Con esta información se procede a verificar la firma del acta. Si la firma es válida, se procesa el acta para obtener los valores de resultados de las actas mediante ICR, de otro modo se registra en el ledger de actas como un acta invalida. Una vez obtenido los valores, estos son registrados en el ledger de resultados, en el cual se adjunta los valores del acta y el ID de la última acta que actualizó los resultados.

El diseño de la app cliente en el cdad debe estar enfocada a eventos, es decir cada vez que se escaneé un acta, esta debe ser inmediatamente enviada hacia en centro de datos. Una consideración importante que sale del alcance del presente proyecto es la integración de la app cliente con el escáner, es de vital importancia tener control sobre estos dos dispositivos, ya que los datos recibidos del escáner al computado no están controlados y se podría enviar datos desde un escáner no autorizado a un computador autorizado.

Cada acta ingresada al centro de datos es almacenada en la red privada de IPFS, en donde se distribuye en bloques y almacena procurando versionamiento, ya que pueden existir varias versiones de la misma acta, por razones de reconteo u otra inconsistencia dentro de la misma.

Los documentos como las actas firmadas o las tablas de resultados podrán ser consultadas mediante una app web hacia la red de IPFS, la cual se va actualizando en tiempo real.

Para poder regir la lógica de negocio debemos analizar cómo están incorporadas los contratos inteligentes identidad, actas, resultados y las funciones que se ejecutan dentro de la app gateway.

El contrato inteligente que rige la lógica y las reglas para interactuar con el ledger de identidad es *SmartContractIdentidad.* A continuación, se detalla el diagrama de clase.

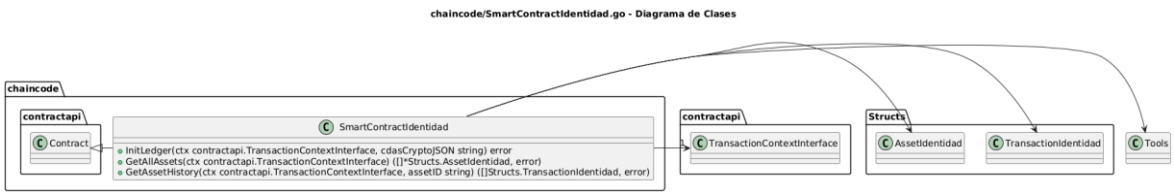


Ilustración 2.2.5 Diagrama de clase SmartContractIdentidad

Este contrato inteligente tiene 3 funciones las cuales se detallan a continuación:

- InitLedger: Esta función se encarga de almacenar los registros de la identidad de los dispositivos digitalizadores de actas. Es la única función de escritura en el ledger.
- GetAllAssetHistory: Esta función retorna todos los assets almacenados dentro de la red de blockchain
- GetAssetHistory: Esta función retorna el asset en base a un identificar dado como parámetro

En este contrato inteligente existe únicamente tres funciones, esto se debe a que dentro del flujo de trabajo no existe funciones de eliminar un escáner, ya que los escáneres iniciales son los acordados para enviar actas digitalizadas.

En este contrato inteligente existe únicamente tres funciones debido a que dentro del flujo de trabajo no existe escenarios en el cual se deba eliminar un escáner, únicamente existe el registro inicial y lectura de datos. Los escáneres registrados inicialmente representan un compromiso y en caso de fallas debería considerarse escáneres de respaldo en cada centro de digitalización de actas electorales y juntas provinciales.

El contrato inteligente que rige la lógica y las reglas para interactuar con el ledger de actas es *SmartContracActas.* A continuación, se detalla el diagrama de clase.

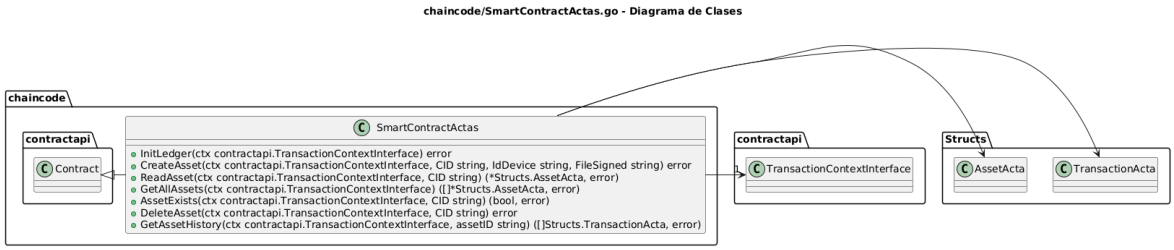


Ilustración 2.2.6 Diagrama de clase SmartContracActas

Este contrato inteligente cuenta con 7 funciones las cuales se detallan a continuación:

InitLedger: Inicia el ledger con valores por defecto.

CreateAsset: Mediante los parámetros dados referentes a un acta, crea el registro de un asset dentro del ledger de actas.

ReadAsset: Mediante un identificador dado como parámetro retorna el asset relacionado.

GetAllAssets: Retorna todos los assets actualmente registrados en la red blockchain.

AssetExists: Verifica la existencia de un asset dentro de la red de blockchain

DeleteAsset: Elimina el Asset de la red de blockchain

GetAssetHistory: Retorna todas las transacciones realizadas en base a un identificador dado como parámetro.

En este contrato inteligente se implementan funciones de lectura, escritura y eliminación debido a que existen escenarios en los cuales se deba anular un acta por inconsistencia numérica. La misma función de CreateAsset funciona para los escenarios de registrar una nueva acta y actualizar la misma.

El contrato inteligente que rige la lógica y las reglas para interactuar con el ledger de resultados es *SmartContracResultados.* A continuación, se detalla el diagrama de clase.

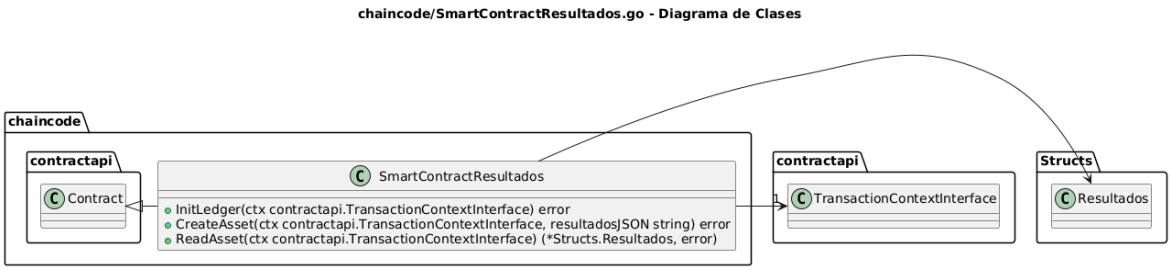


Ilustración 2.2.7 Diagrama de clase SmartContracResultados

Este contrato inteligente cuenta con tres funciones, las cuales se detallan a continuación:

InitLedger: Inicializa un asset de resultados con valores nulos.

CreateAsset: Registra un nuevo asset en el ledger de Resultados. Esta función es la única de escritura.

ReadAsset: Mediante un identificador dado como parámetro retorna el asset relacionado.

En este contrato inteligente se tiene únicamente dos funcionalidades escribir y leer. Se considera que cada nuevo registro de resultados va a ser afectado por los resultados de un acta, con lo cual si se ingresa resultados de un acta procesada previamente que fue invalidada, a la interna se procesa los cambios mediante el registro de la diferencia entre las dos actas involucradas.

Los elementos que integran un peer a nivel de aplicaciones se explica a continuación:

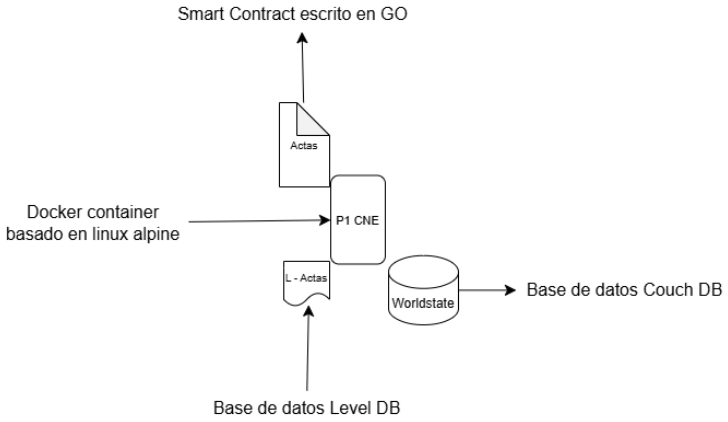


Ilustración 2.2.8 Composición de apps de un peer

Las aplicaciones que integra un peer esencialmente son tres, las cuales se detallan a continuación:

Peer Docker container: El contenedor Docker es en sí el peer donde se almacena y ejecuta el contrato inteligente, así como las bases de datos para el ledger y worldstate, la base de datos de los assets.

Base de datos Level DB: Level DB es una base de datos rápida y sencilla. Los registros que almacena se basan en clave-valor. Funciona perfecto para registrar los eventos y transacciones que se componen en tracción id – cuerpo de la transacción.

Base de datos Couch DB: Couch DB es una base de datos NoSQL la cual permite almacenar datos estructurados y realizar consultas avanzadas mediante solicitudes HTTP. Dentro de esta base de datos se almacena los assets que se han manipulado mediante las transacciones realizadas en la red de Hyperledger. Cabe recalcar que esta base de datos puede ser vaciada, no obstante, al contar con el ledger inmutable puede ser reconstruida siguiendo las transacciones en el orden de encadenamiento de estas.

SmartContract: El contrato inteligente o SmartContract puede ser escrito en diferentes lenguajes como JavaScript o Golang. Para el presente proyecto se escogió el lenguaje Golang. Este contrato inteligente es compilado, empaquetado y alojado para ser ejecutado dentro del peer, el cual se encuentra a la espera del llamado de una función especificada en el contrato inteligente.

Finalmente, el proyecto queda estructurado de la siguiente forma:

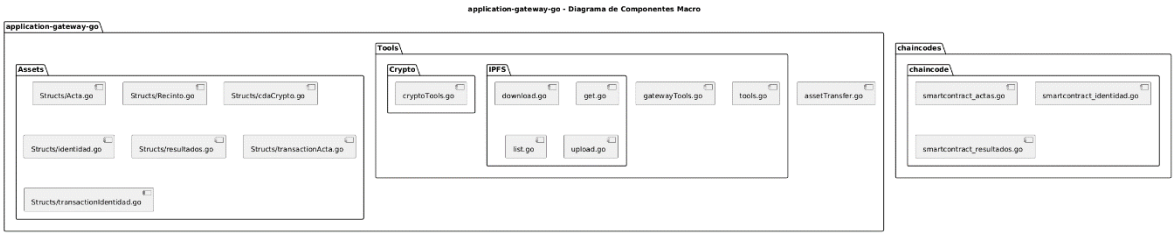


Ilustración 2.2.9 Estructuración de proyecto

En la ilustración 2.2.9 se puede visualizar como se encuentra estructurado el proyecto. Dentro del directorio Assets se encuentra alojado los modelos usados para abstraer las estructuras de datos utilizadas. Dentro del directorio Tools se encuentran funcionalidades utilizadas para generar material criptográfico, firma de ficheros, creación de la conexión con el Gateway, entre otras más. Dentro del directorio chaincodes se aloja el chaincode que contiene los contratos inteligentes.

2.3 Desarrollo de prototipo

Para desarrollar el diseño empleado dentro del presente proyecto se formuló un prototipo, el cual muestra las funcionalidades básicas de todo el Sistema Informático de Escrutinios y Resultados. El entorno de desarrollo se describe a continuación:

- Máquina virtual Linux Ubuntu 24.04 LTS virtualizada sobre VMware WorkStation Pro
- Todos los nodos dentro de la infraestructura como puede ser las entidades certificados, *peers* y ordenadores son emulados mediante contenedores, de tal forma que la red interna y todo el prototipo funciona dentro de la máquina virtual preconfigurada.
- Los prerrequisitos necesarios como la instalación de Docker y Golang, entre otros se detalla en el anexo I.
- Consideraciones básicas respecto a hardware de la máquina virtual se describe en la siguiente imagen:

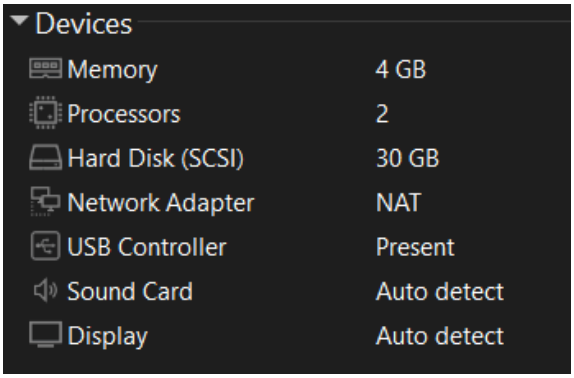


Ilustración 2.3.1 Configuraciones de hardware de máquina virtual

El prototipo no implementa interfaces web para el acceso o envío de información. El alcance del presente proyecto refiere únicamente a la infraestructura interna y su funcionamiento. Razón por la cual la interacción con la aplicación Gateway se hace directo mediante interface de línea de comandos, *CLI* por sus siglas en inglés.

A continuación, se presenta la arquitectura usada para el registro de identidad de los dispositivos. Por limitaciones el envío de los ficheros se hace mediante una **interfaz** de CLI

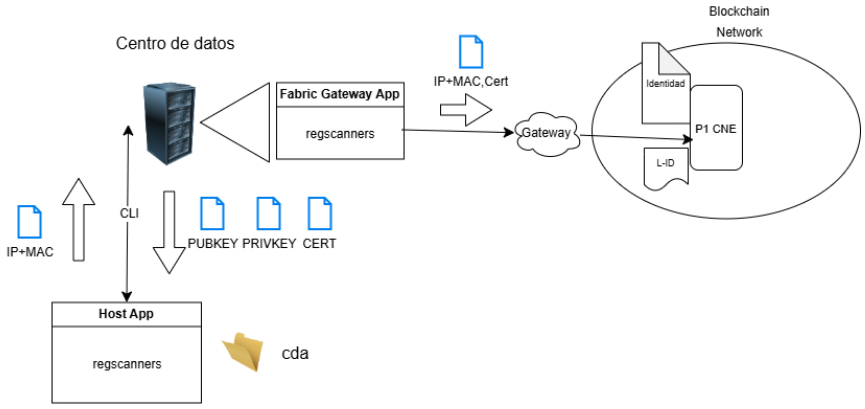


Ilustración 2.3.2 Arquitectura prototipo – registro de cdads

Para emular el envío de información de los dispositivos se creó la función *makedirs* la cual genera una estructura de datos con ficheros que identifican un computador scanner. A continuación, muestra la estructura de carpetas mencionada.

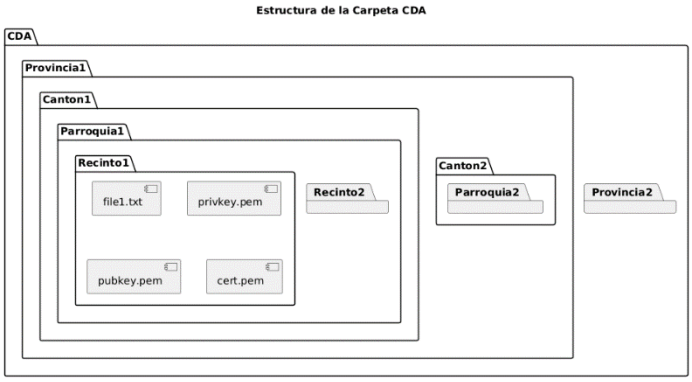


Ilustración 2.3.3 Estructura de directorios para cda

En la figura anterior se muestra file1.txt, el cual es el fichero que contiene el dato de IP; MAC. La cantidad de ficheros que se crea está controlada por las entradas dentro del fichero Assets/cda.txt.

Una vez creado el material se puede hacer uso de la función *regscanners,* la cual tomará la información alojada dentro de la estructura de carpetas y las procesará de acuerdo con el esquema diseñado.

A continuación, se muestra un diagrama de secuencia de la función.

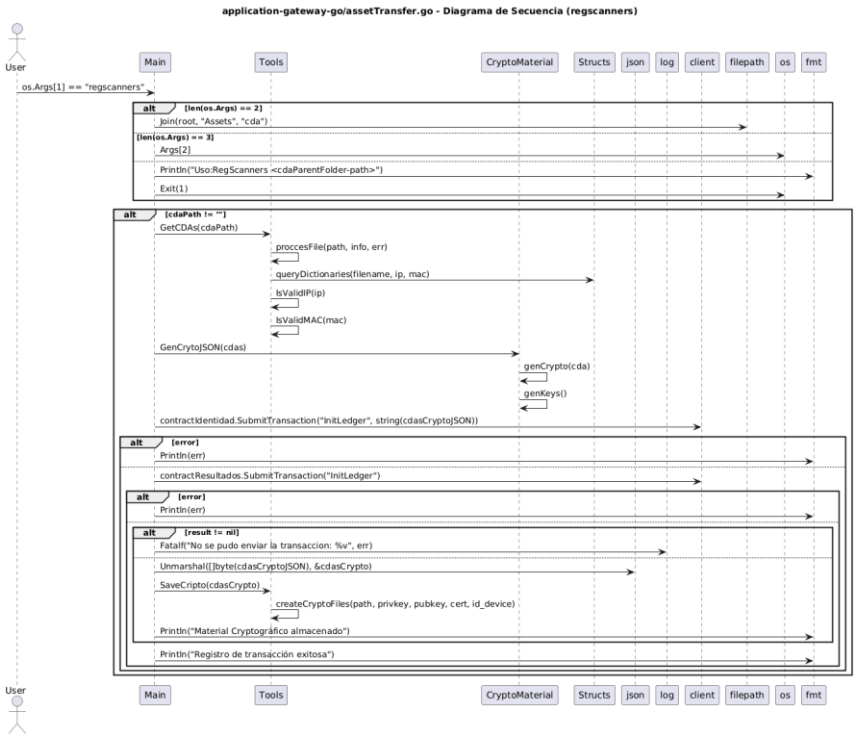


Ilustración 2.3.4 Diagrama de secuencia función regscanners

Una vez registrado los cdad se puede proceder al escaneo de las actas.

La arquitectura implementada en el prototipo para el proceso de escrutinio y publicación de actas se describe a continuación:

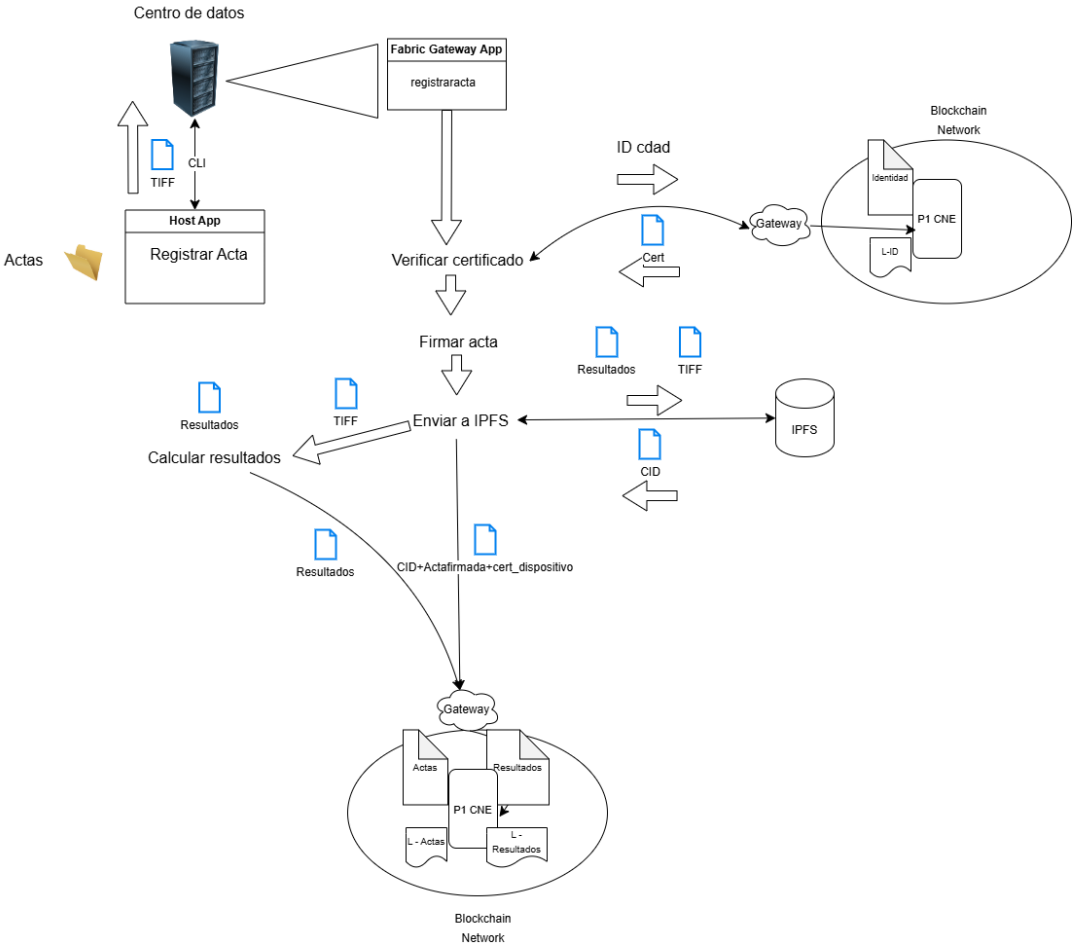


Ilustración 2.3.5 Arquitectura prototipo – Registro de actas

Dentro del directorio Assets/Actas se encuentra una serie de actas en formato TIFF, estas actas fueron obtenidas de la página del CNE y serán usadas para la ejecución del prototipo.

Mediante línea de comandos se puede hacer uso de la función *registraracta,* esta función tomará un acta de prueba y realizará el procesamiento emulando el envío de un cdad, para ello recupera la llave privada asociada al acta, firma el documento y registra el acta tanto en IPFS como en la red blockchain. La relación entre acta y cdad se da por su nombre. Tanto el cdad como el acta siguen el patrón *Provincia.Canton.Parroquia.Recinto* el cual se encuentra respectivamente codificado de acuerdo a la correspondencia descrita en el documento obtenido desde la página web del CNE [28]. Para obtener el documento revisar el anexo II.

A continuación, se muestra un diagrama de secuencia de la función:

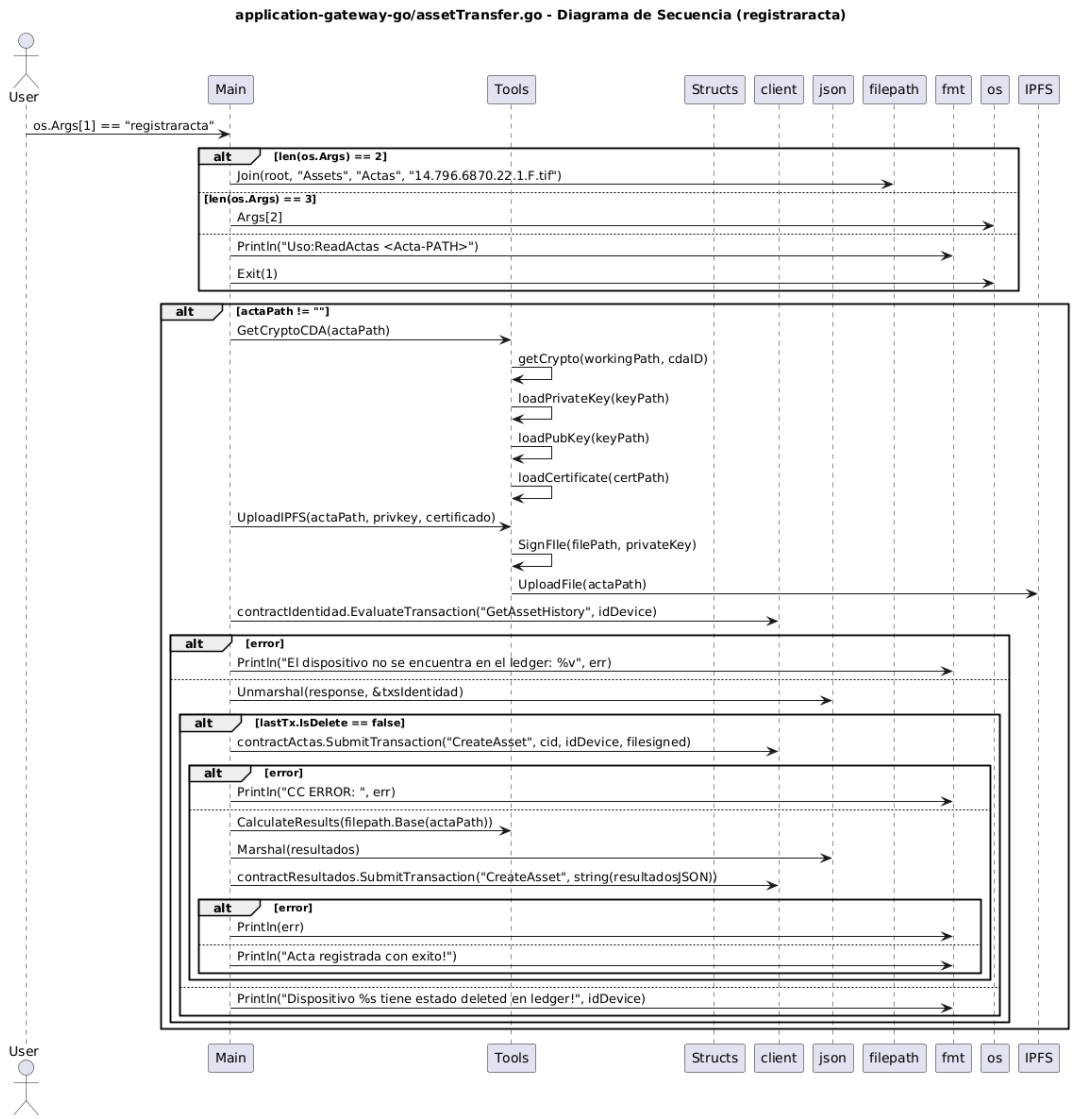


Ilustración 2.3.6 Diagrama de secuencia función registraracta

Las tres funciones descritas anteriormente son las principales en cuanto al uso del prototipo. Para revisar código, diagramas de clase y de secuencia de las funciones internas, así como el resto de las funciones principales del prototipo dirigirse a la sección de anexos.

Finalmente, el menú presentado en el prototipo se encuentra estructurado de la siguiente forma, para poder ilustrar el flujo de trabajo se presenta el siguiente diagrama de secuencia:

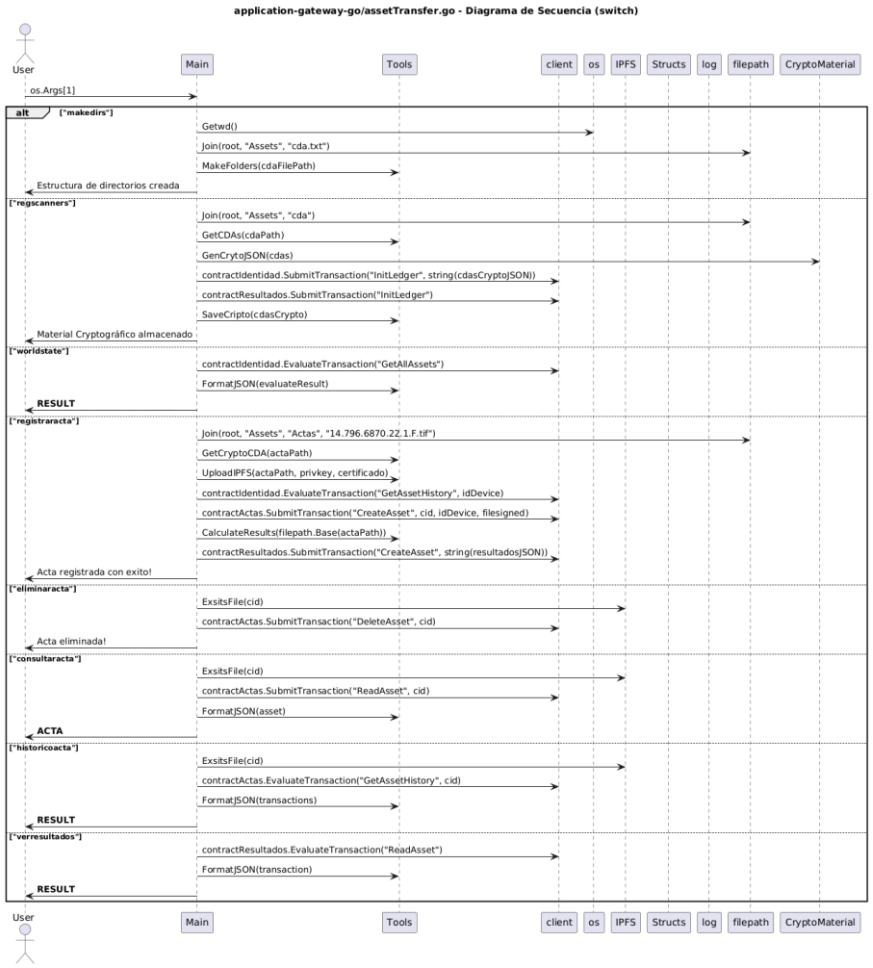


Ilustración 2.3.7 Diagrama de secuencia función main

El prototipo se encuentra alojado en un repositorio público de GitHub desde donde puede ser descargado y probado. Las instrucciones para iniciar se encuentran descritas en el anexo XYZ.

3 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

Dado que la implementación no puede ser desplegada en un entorno de producción el apartado de pruebas no se ha considerado. Dentro de la implementación se detalló las pruebas de concepto mediante la implementación de funciones que simulen el comportamiento de un entorno de producción. Los resultados de las pruebas de concepto reflejaron funcionalidad de lo descrito en el apartado de diseño. No se documenta el apartado de pruebas debido a la trivialidad de los resultados.

3.1 Resultados

En el presente trabajo de integración curricular se exploró la implementación actual que mantiene el Consejo Nacional Electoral en el Sistema Informático de Escrutinios y

Resultado, el análisis realizado sobre la situación actual permitió comprender las oportunidades de mejora en las cuales se puede implementar una solución y dar pie al desarrollo del proyecto actual.

Mediante las pruebas de concepto realizadas sobre el prototipo final se pudo evidenciar la funcionalidad de cada uno de los componentes (infraestructura, almacenamiento y aplicación) que conforman el presente proyecto. Adicional, se evidenció la viabilidad de incorporar un sistema descentralizado al SIER del CNE. Descentralizar el proceso de tratamiento de actas para el escrutinio, así como la publicación de resultados presenta cambio significativo en el ámbito de transparencia y control. Agregar figuras de control del gobierno y agentes internacionales al sistema es un medio en el cual se garantiza la regulación del proceso, así como la satisfacción de los resultados, ya que la responsabilidad y compromiso del procesamiento de las actas electorales es compartido.

3.2 Conclusiones

Para poder delimitar el presente proyecto y componente se establecieron objetivos de los cuales, a continuación, se detalla las conclusiones obtenidas luego del desarrollo:

- Analizar el sistema de escrutinios y publicación de resultados que utiliza el CNE: Actualmente, el Consejo Nacional Electoral mantiene el SIER, en el cual los datos se encuentran alojados en servicios de terceros y no permite tener control y trazabilidad de las acciones que se realicen sobre cada acta y resultado generado en un proceso electoral. La combinación del sistema de interconexión de datos SID, junto con el Sistema Informático de Escrutinios y Resultados SIER, y la adopción de tecnologías propuestas en el presente TIC, puede brindar una oportunidad de transparentar el proceso electoral. La transparencia en el proceso electoral es un pilar fundamental dentro de la democracia del país, de otro modo las y los ciudadanos serán reacios a sus gobernantes y dirigentes.

- Analizar los requerimientos funcionales y legales del proceso de escrutinios y publicación de resultados: El Consejo Nacional Electoral en el año 2016 certificó sus procesos electorales con la norma ISO/TS 17582:2014, lo cual garantiza que los procesos cumplen lineamientos de calidad y se encuentran dentro del margen de la democracia, lo cual en el ámbito operativo es real. El proceso de logística y despliegue de infraestructura en un proceso de elección de autoridades se encuentra respaldado por la norma. No obstante, existe elementos que no cubre la norma y que debería ser controlado, como es el caso del sistema de escrutinio y publicación de resultados. La infraestructura puede encontrarse implementada, sin

embargo, si no existe un correcto uso, no se obtiene los resultados transparentes y esperados. En el país existen normativas legales que obligaron al CNE a implementar los sistemas SIER y SID, e inclusive realizar un proceso de auditoría al proceso de Elecciones del año 2019 lo cual denota la necesidad de tener mecanismos de control e involucrar a las entidades de control de gobierno e internacionales, de tal forma que garanticen que el proceso electoral de elecciones de autoridades sea transparente y descentralizado.

- Diseñar la infraestructura tecnológica del sistema de cadena de bloques para el registro de las actas de escrutinio y resultados electorales: Mediante el diseño y prototipado se pudo evidenciar la viabilidad de implementar un sistema descentralizado permisionado dentro del sistema actual SIER del CNE, a pesar de que este diseño no se encuentre dentro del presente componente, se encuentra realizado a nivel de proyecto ya que fue migrado hacia otro componente. Incorporar Hyperledger Fabric al sistema actual SIER del CNE traería trazabilidad de las transacciones realizadas con las actas de resultados. Implementar trazabilidad completa traería ventajas en cuanto al control y manejo de cambios dentro del proceso de escrutinio y publicación de resultados. Al contar con una red permisionada, se podría evitar escenarios de fraude ya que en primera instancia este agente fraudulento debió ser admitido, de donde esta acción y todas las realizadas dentro de la red quedarían registradas.

- Diseñar los contratos inteligentes y la aplicación para registrar las transacciones relacionadas al proceso de escrutinios y publicación de resultados: Dentro del presente componente se diseñó y se realizó el prototipo de tres contratos inteligentes los cuales rigen la lógica de lectura y escritura de los registros inmutables. Los tres contratos inteligentes son fundamentales dentro del proceso de escrutinio y publicación de resultados ya que el registro inmutable asociado almacena datos vitales para el ejercicio de auditorías sobre elecciones posteriores a la implementación de Hyperledger Fabric.

- Desarrollar el prototipo del sistema de cadena de bloques: El desarrollo del prototipo fue realizado de forma completa y exitosa. Se pudo integrar los componentes realizados por cada integrante del proyecto, de donde se pudo evidenciar la viabilidad de integrar sistemas descentralizados tanto para almacenamiento de ficheros, así como el almacenamiento descentralizado del registro de transacciones y la viabilidad de implementar una red sobre el proyecto de Hyperledger Fabric.

Los objetivos específicos fueron cumplidos y desarrollados con lo cual se garantiza que el objetivo general de diseñar un sistema que garantice la integridad e inmutabilidad de las actas de escrutinio digitalizadas y de los resultados electorales ha sido cumplido, evidenciando puntos de mejora al sistema actual SIER del CNE.

3.3 Recomendaciones

- Se recomienda que, no se use el prototipo en entornos de pruebas. Las funciones realizadas dentro del prototipo fueron creadas para demostrar las capacidades de la propuesta dada en la fase de diseño, con lo cual implementar un ambiente de producción basado en el prototipo no garantiza un entorno seguro y con resultados esperados.
- El compromiso de las entidades involucradas en el diseño del sistema descentralizado es vital ya que el proceso electoral actual en ecuador se encuentra dividido en la parte física y la parte digital. Se recomienda que, se debe acordar un compromiso legal para registrar los computadores escáner. De otro modo queda a discreción el uso de la entidad certificadora, con lo cual se pierde credibilidad y confianza en los miembros de la red de blockchain.

4 REFERENCIAS BIBLIOGRÁFICAS

[1] Asamblea Nacional Del Ecuador, «Ley Organica Reformatoria a la Ley Organica Electoral y de Organizaciones Politicas, Codigo de la Democracia,» 03 Febrero 2020. [En línea]. Available: https://reformaspoliticas.org/wp-content/uploads/2020/07/Reformas-CD-2020.pdf. [Último acceso: 08 Julio 2024].

[2] Consejo Nacional Electoral, «Las auditorías al sistema informático del CNE se realizarán una vez concluido el proceso electoral,» [En línea]. Available: https://www.cne.gob.ec/las-auditorias-al-sistema-informatico-del-cne-se-realizaran-una-vez-concluido-el-proceso-electoral/.

[3] Teleamazonas, «Tecnología blockchain en las actas de las elecciones de Ecuador 2023,» Teleamazonas, 2023. [En línea]. Available: https://www.teleamazonas.com/blockchain-tecnologia-elecciones-seccionales-2023/. [Último acceso: 09 Julio 2024].

[4] Zeyo, «Blockchain en elecciones seccionales de Ecuador,» 7 Febrero 2023. [En línea]. Available: https://zeyo.io/casos-de-exito/blockchain-en-elecciones-seccionales-de-ecuador/. [Último acceso: 1 Mayo 2024].

[5] International Organization for Standardization, ISO/TS 17582:2014 - Quality management systems -- Particular requirements for the application of ISO 9001:2008 for electoral organizations at all levels of government., 2014.

[6] Hyperledger, «Introducción,» 2020. [En línea]. Available: https://hyperledger-fabric.readthedocs.io/es/latest/whatis.html.

[7] G. Coulouris, J. Dollimore, T. Kindberg y G. Blair, Distributed Systems: Concepts and Design, Addison-Wesley, 2012.

[8] M. Pilkington, Blockchain Technology: Principles and Applications.

[9] F. D. A. Lopez Fuentes, Sistemas distribuidos, Unidad Cuajimalpa: D.R. © 2015 UNIVERSIDAD AUTÓNOMA METROPOLITANA , 2015.

[10] A. S. Tanenbaum y M. Van Steen, Distributed Systems: Principles and Paradigms, Prentice-Hall, 2007.

[11] M. A. El Khaddar, Middleware Architecture, doi: 10.5772/intechopen.92536., 2021.

[12] W. Stalling, Operating Systems: Internals and Design Principles, 2018.

[13] T. Erl, R. Khattak y P. Buhler, Cloud Computing: Concepts, Technology & Architecture, Prentice Hall, 2013.

[14] Protocol Labs, «IPFS Documentatio,» [En línea]. Available: https://docs.ipfs.io.

[15] A. Narayanan, J. Bonneau, E. Felten, A. Miller y S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, 2016.

[16] R. S. y. M. P. L. Lamport, «The Byzantine Generals Problem,» *ACM Transactions on Programming Languages and Systems,* pp. 382-401, 1982.

[17] Digiconomist, «Bitcoin Energy Consumption Index,» [En línea]. Available: https://digiconomist.net/bitcoin-energy-consumption.

[18] D. Tapscott y A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 2016.

[19] M. Cas y P. Vigna, The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order.

[20] I. Bashir, Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, 2018.

[21] N. Szabo, The Idea of Smart Contracts, 1997.

[22] C. Cachin, Architecture of the Hyperledger Blockchain Fabric, 2016.

[23] E. Androulaki, C. Cachin, C. Ferris, M. Sethi y C. Stathakopoulou, Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains, 2018.

[24] Consejo Nacional Electoral, «Rendición de cuentas 2023,» [En línea]. Available: https://www.cne.gob.ec/rendicion-de-cuentas-2023/.

[25] Consejo Nacional Electoral, «OEA otorgó oficialmente Certificación Internacional ISO al CNE de Ecuador,» [En línea]. Available: https://www.cne.gob.ec/oea-otorgo-oficialmente-certificacion-internacional-iso-al-cne-de-ecuador/.

[26] Hyperledger, «Hyperledger Fabric Model,» [En línea]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.5/fabric_model.html.

[27] Hyperledger Fabric Docs, «How Fabric networks are structured,» Hyperledger 2020-2023, 2023. [En línea]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.5/network/network.html. [Último acceso: 01 Mayo 2024].

[28] Consejo Nacional Electoral, «Delegado de Centro de Digitalización de Actas 1,» 6 Abril 2024. [En línea]. Available: https://www.cne.gob.ec/download/delegado-de-centro-de-digitalizacion-de-actas-1/. [Último acceso: 1 Agosto 2024].

[29] L. Carvajal, Metodología de la Investgación Científica. Curso general y aplicado, 28 ed., Santiago de Cali: U.S.C., 2006, p. 139.

[30] El Universo, «Las denuncias de 'fraude' han sido una constante en los procesos electorales del Ecuador,» *El Universo,* 01 Marzo 2021.

[31] R. Digital, «Detectan supuesto centro de cómputo en el CNE Guayas donde se imprimía actas no oficiales,» *TC Television,* 09 Febrero 2023.

[32] EL Universo, «El CNE esta sin recursos para cambios tecnológicos,» 20 Enero 2020. [En línea]. Available: https://www.pressreader.com. [Último acceso: 08 Julio 2024].

[33] teleamazonas, «Tecnología blockchain en las actas de las elecciones de Ecuador 2023,» 5 Febrero 2023. [En línea]. Available: https://www.teleamazonas.com/blockchain-tecnologia-elecciones-seccionales-2023/. [Último acceso: 1 Agosto 2024].

[1] Asamblea Nacional Del Ecuador, «Ley Organica Reformatoria a la Ley Organica Electoral y de Organizaciones Politicas, Codigo de la Democracia,» 03 Febrero 2020. [En línea]. Available: https://reformaspoliticas.org/wp-content/uploads/2020/07/Reformas-CD-2020.pdf. [Último acceso: 08 Julio 2024].

[2] Consejo Nacional Electoral, «Las auditorías al sistema informático del CNE se realizarán una vez concluido el proceso electoral,» [En línea]. Available: https://www.cne.gob.ec/las-auditorias-al-sistema-informatico-del-cne-se-realizaran-una-vez-concluido-el-proceso-electoral/.

[3] Teleamazonas, «Tecnología blockchain en las actas de las elecciones de Ecuador 2023,» Teleamazonas, 2023. [En línea]. Available: https://www.teleamazonas.com/blockchain-tecnologia-elecciones-seccionales-2023/. [Último acceso: 09 Julio 2024].

[4] Zeyo, «Blockchain en elecciones seccionales de Ecuador,» 7 Febrero 2023. [En línea]. Available: https://zeyo.io/casos-de-exito/blockchain-en-elecciones-seccionales-de-ecuador/. [Último acceso: 1 Mayo 2024].

[5] International Organization for Standardization, ISO/TS 17582:2014 - Quality management systems -- Particular requirements for the application of ISO 9001:2008 for electoral organizations at all levels of government., 2014.

[6] Hyperledger, «Introducción,» 2020. [En línea]. Available: https://hyperledger-fabric.readthedocs.io/es/latest/whatis.html.

[7] G. Coulouris, J. Dollimore, T. Kindberg y G. Blair, Distributed Systems: Concepts and Design, Addison-Wesley, 2012.

[8] M. Pilkington, Blockchain Technology: Principles and Applications.

[9] F. D. A. Lopez Fuentes, Sistemas distribuidos, Unidad Cuajimalpa: D.R. © 2015 UNIVERSIDAD AUTÓNOMA METROPOLITANA , 2015.

[10] A. S. Tanenbaum y M. Van Steen, Distributed Systems: Principles and Paradigms, Prentice-Hall, 2007.

[11] M. A. El Khaddar, Middleware Architecture, doi: 10.5772/intechopen.92536., 2021.

[12] W. Stalling, Operating Systems: Internals and Design Principles, 2018.

[13] T. Erl, R. Khattak y P. Buhler, Cloud Computing: Concepts, Technology & Architecture, Prentice Hall, 2013.

[14] Protocol Labs, «IPFS Documentatio,» [En línea]. Available: https://docs.ipfs.io.

[15] A. Narayanan, J. Bonneau, E. Felten, A. Miller y S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, 2016.

[16] R. S. y. M. P. L. Lamport, «The Byzantine Generals Problem,» *ACM Transactions on Programming Languages and Systems,* pp. 382-401, 1982.

[17] Digiconomist, «Bitcoin Energy Consumption Index,» [En línea]. Available: https://digiconomist.net/bitcoin-energy-consumption.

[18] D. Tapscott y A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 2016.

[19] M. Cas y P. Vigna, The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order.

[20] I. Bashir, Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, 2018.

[21] N. Szabo, The Idea of Smart Contracts, 1997.

[22] C. Cachin, Architecture of the Hyperledger Blockchain Fabric, 2016.

[23] E. Androulaki, C. Cachin, C. Ferris, M. Sethi y C. Stathakopoulou, Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains, 2018.

[24] Consejo Nacional Electoral, «Rendición de cuentas 2023,» [En línea]. Available: https://www.cne.gob.ec/rendicion-de-cuentas-2023/.

[25] Consejo Nacional Electoral, «OEA otorgó oficialmente Certificación Internacional ISO al CNE de Ecuador,» [En línea]. Available: https://www.cne.gob.ec/oea-otorgo-oficialmente-certificacion-internacional-iso-al-cne-de-ecuador/.

[26] Hyperledger, «Hyperledger Fabric Model,» [En línea]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.5/fabric_model.html.

[27] Hyperledger Fabric Docs, «How Fabric networks are structured,» Hyperledger 2020-2023, 2023. [En línea]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.5/network/network.html. [Último acceso: 01 Mayo 2024].

[28] Consejo Nacional Electoral, «Delegado de Centro de Digitalización de Actas 1,» 6 Abril 2024. [En línea]. Available: https://www.cne.gob.ec/download/delegado-de-centro-de-digitalizacion-de-actas-1/. [Último acceso: 1 Agosto 2024].

[29] L. Carvajal, Metodología de la Investgación Científica. Curso general y aplicado, 28 ed., Santiago de Cali: U.S.C., 2006, p. 139.

[30] El Universo, «Las denuncias de 'fraude' han sido una constante en los procesos electorales del Ecuador,» *El Universo,* 01 Marzo 2021.

[31] R. Digital, «Detectan supuesto centro de cómputo en el CNE Guayas donde se imprimía actas no oficiales,» *TC Television,* 09 Febrero 2023.

[32] EL Universo, «El CNE esta sin recursos para cambios tecnológicos,» 20 Enero 2020. [En línea]. Available: https://www.pressreader.com. [Último acceso: 08 Julio 2024].

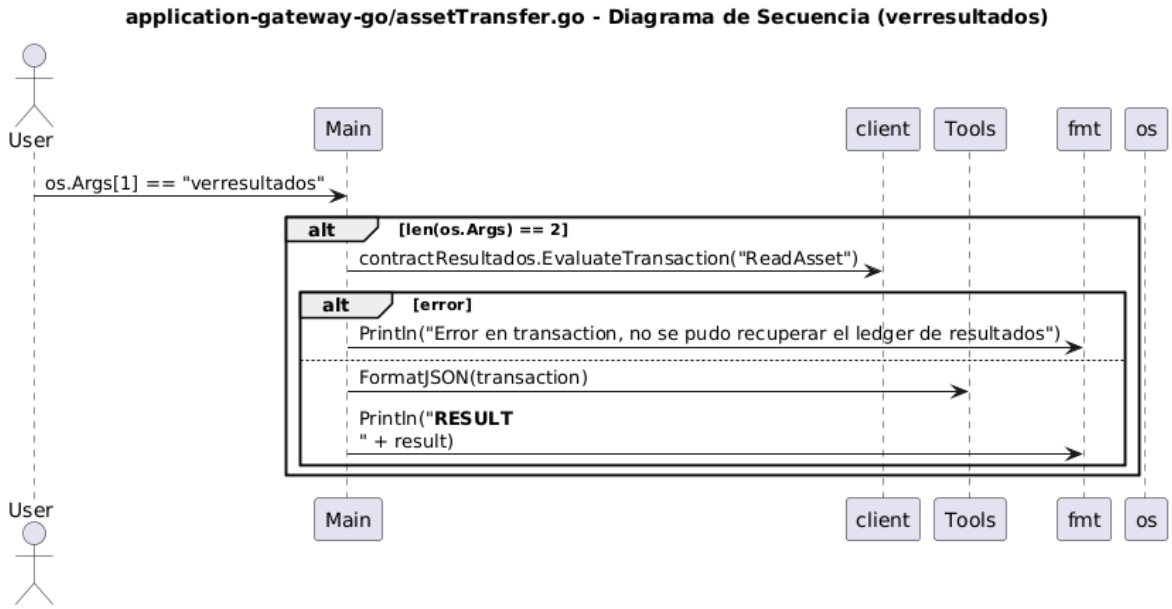
[33] teleamazonas, «Tecnología blockchain en las actas de las elecciones de Ecuador 2023,» 5 Febrero 2023. [En línea]. Available: https://www.teleamazonas.com/blockchain-tecnologia-elecciones-seccionales-2023/. [Último acceso: 1 Agosto 2024].

5 ANEXOS

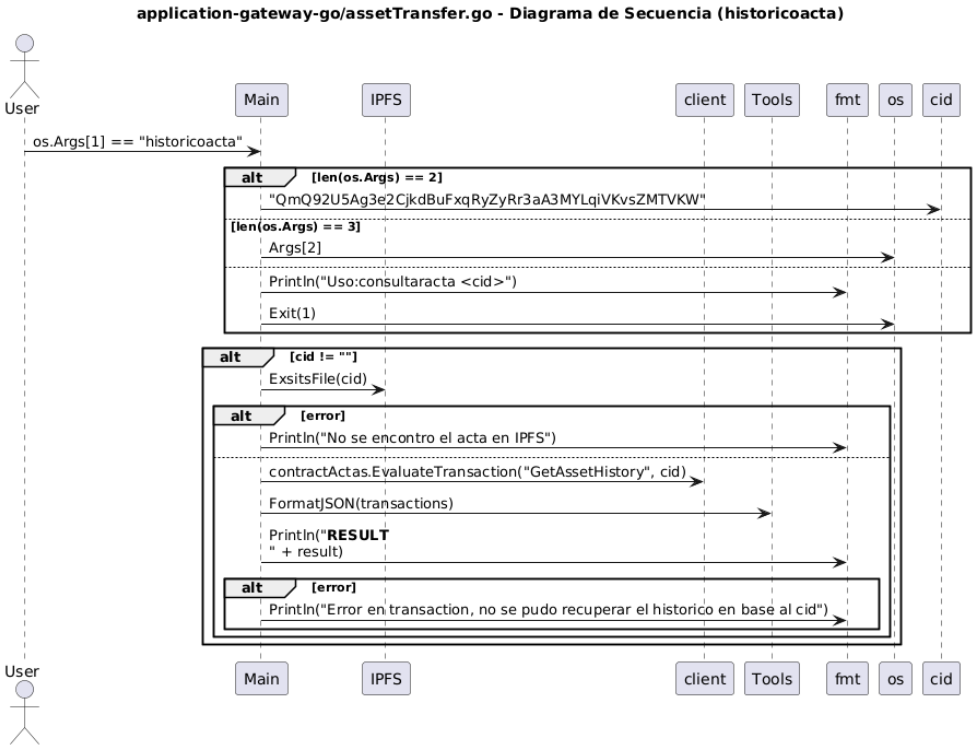
ANEXO I. Instalación de prerrequisitos

ANEXO II. Distribución de recintos electorales

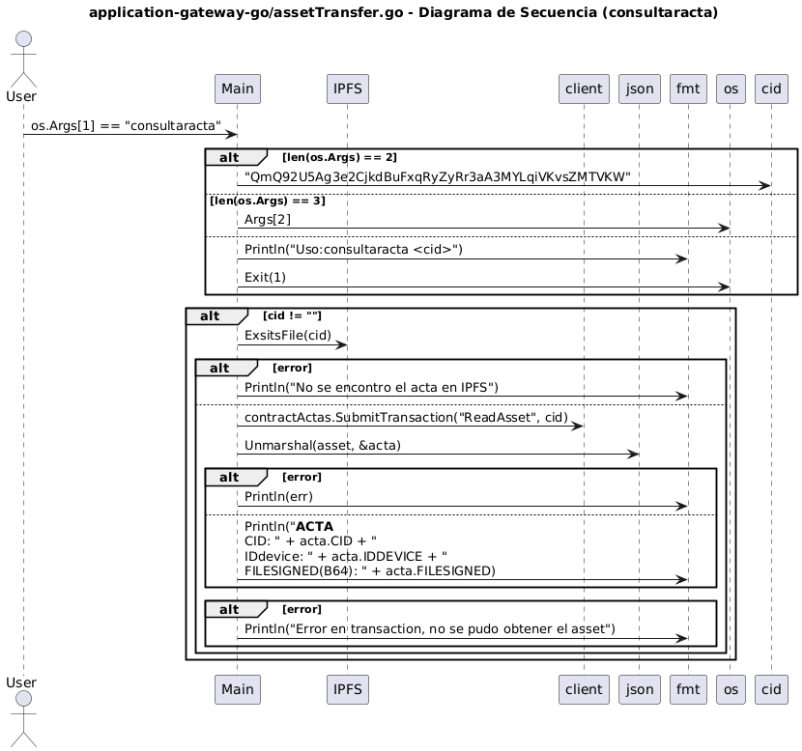
Anexos III. Diagrama de secuencia función verresultados



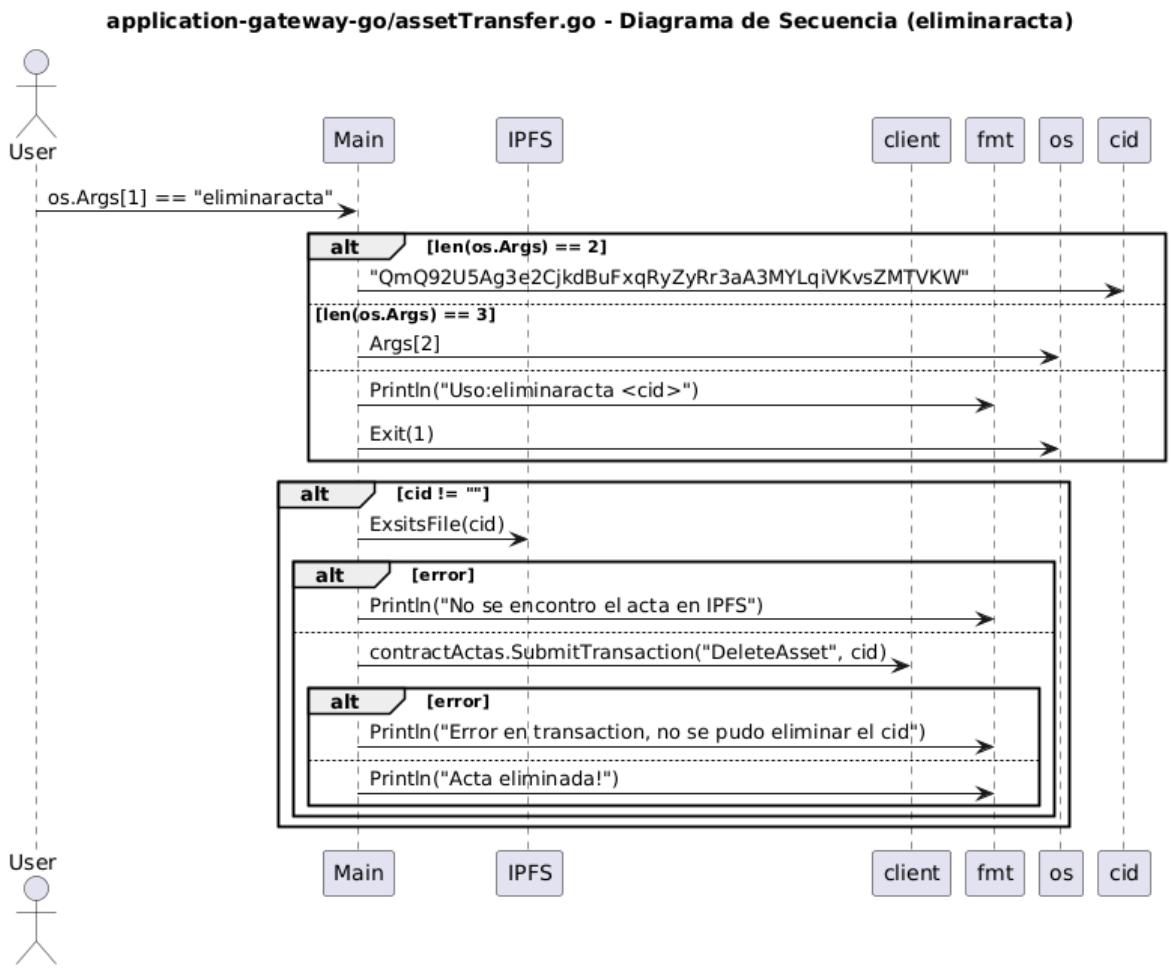
Anexos III. Diagrama de secuencia función historiacta



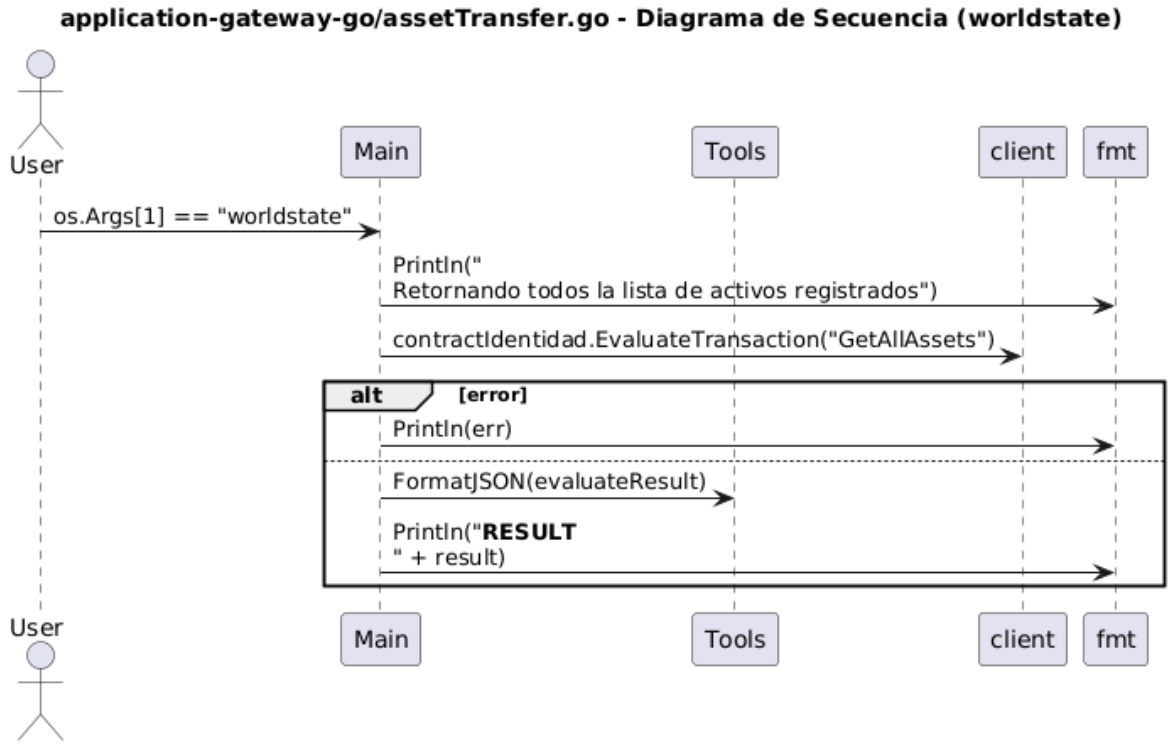
Anexos IV. Diagrama de secuencia función historiacta



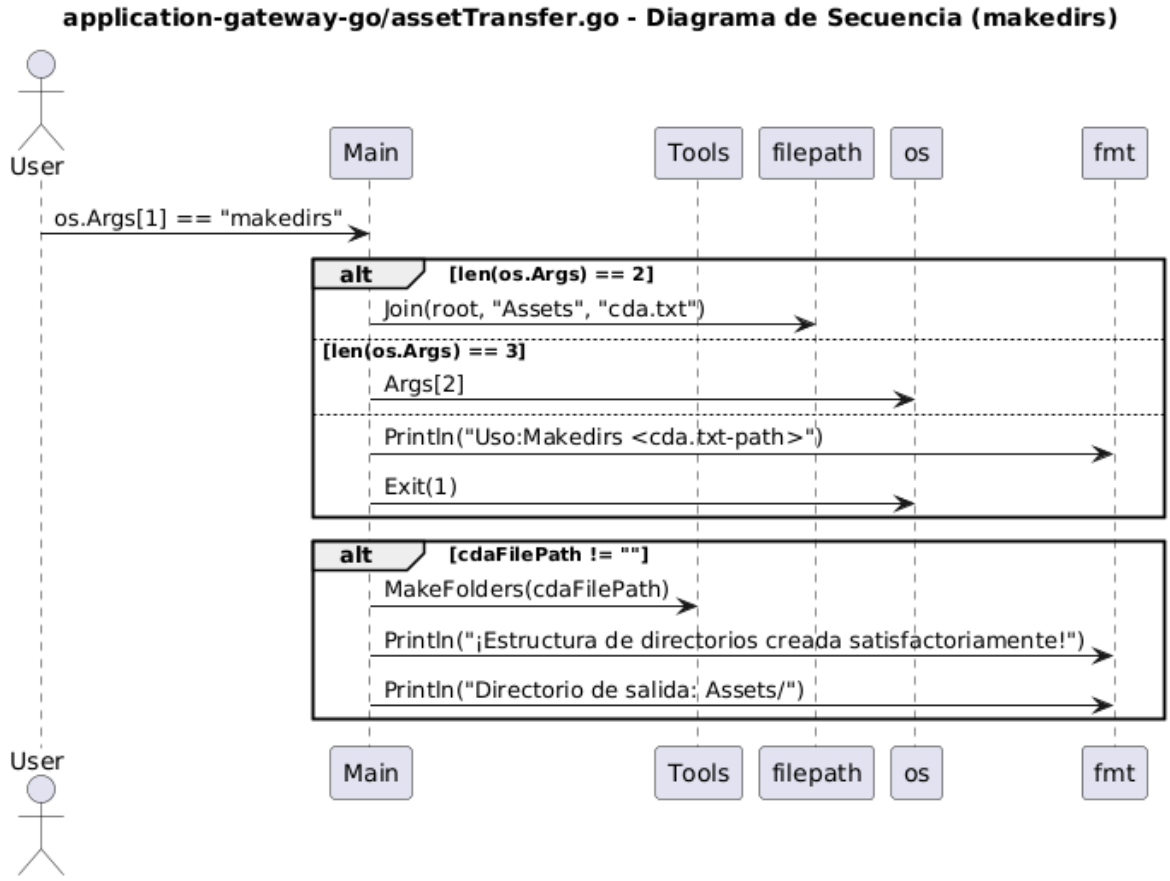
Anexos V. Diagrama de secuencia función eliminaracta



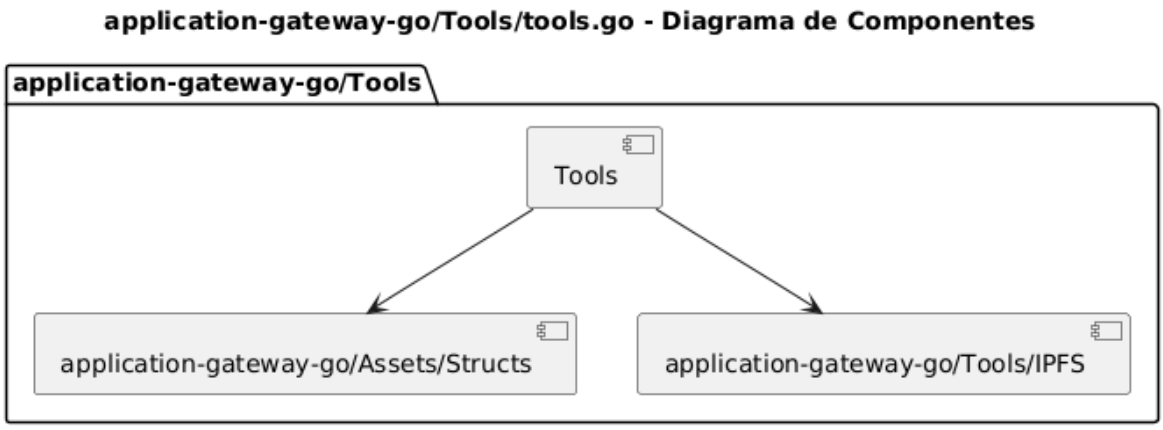
Anexos VI. Diagrama de secuencia función worldstate



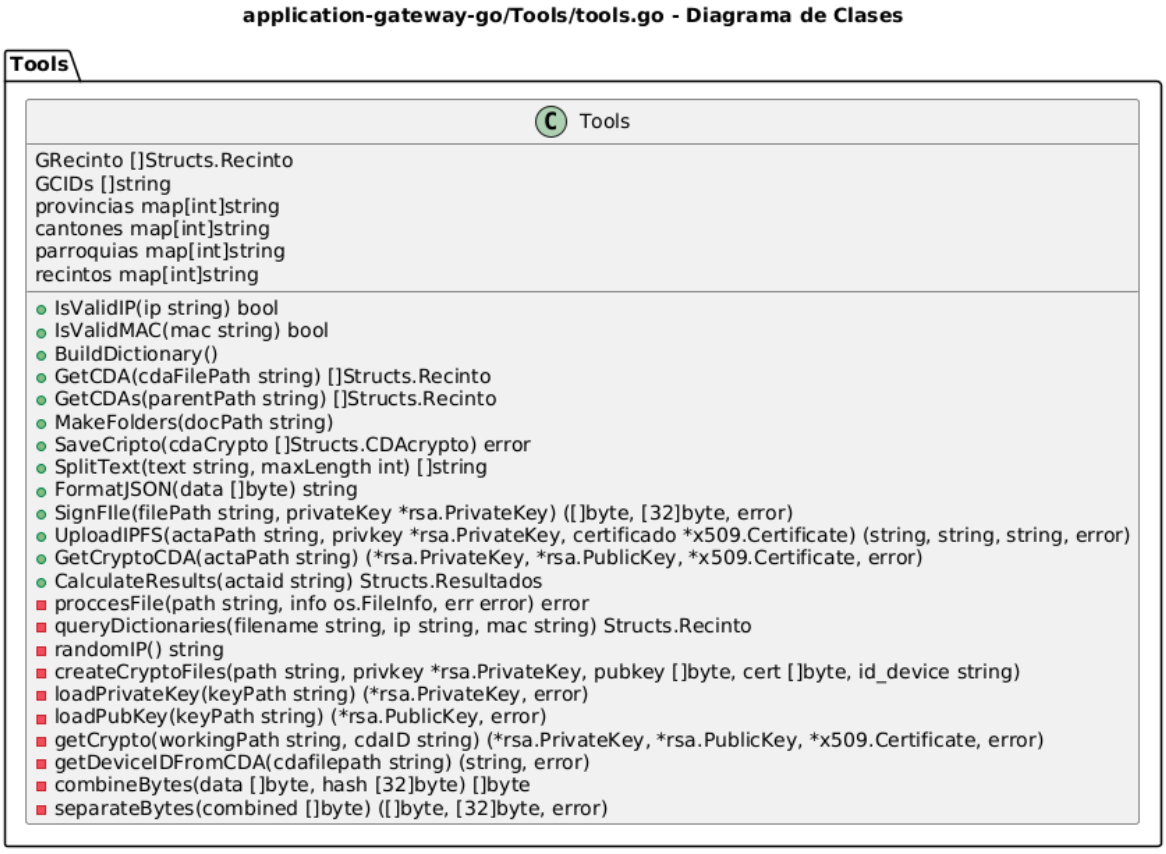
Anexos VII. Diagrama de secuencia función makedirs



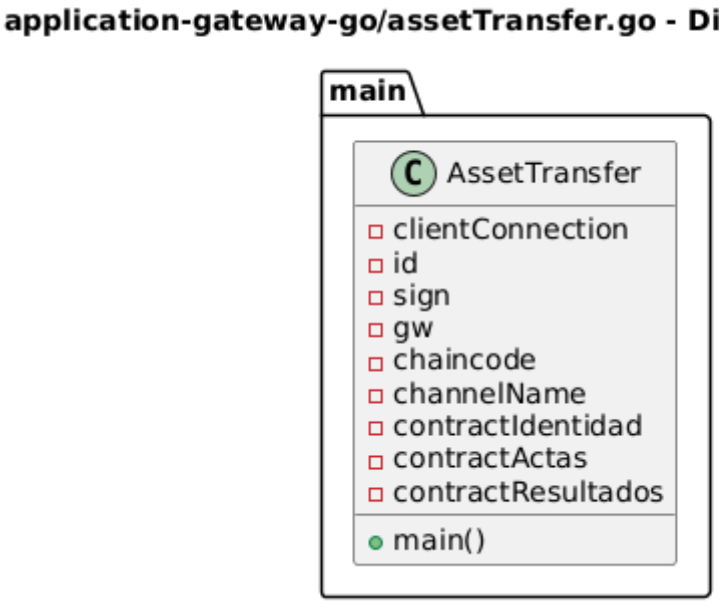
Anexos VIII. Diagrama de componentes módulo Tools



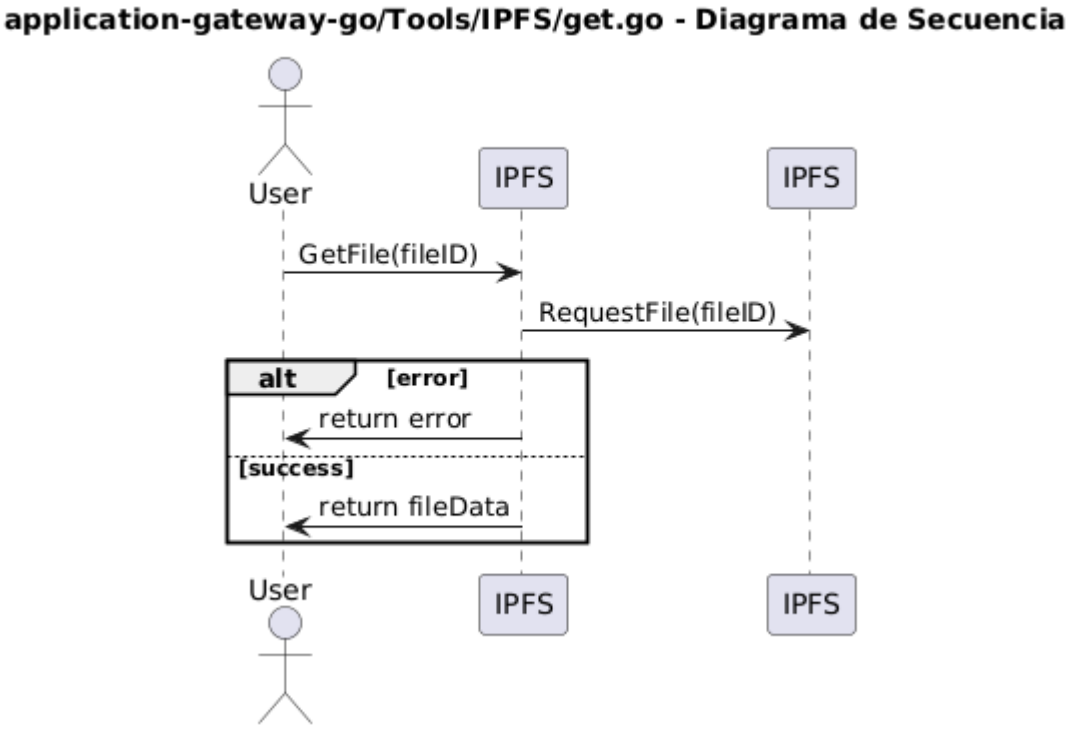
Anexos III. Diagrama de clase módulo Tools



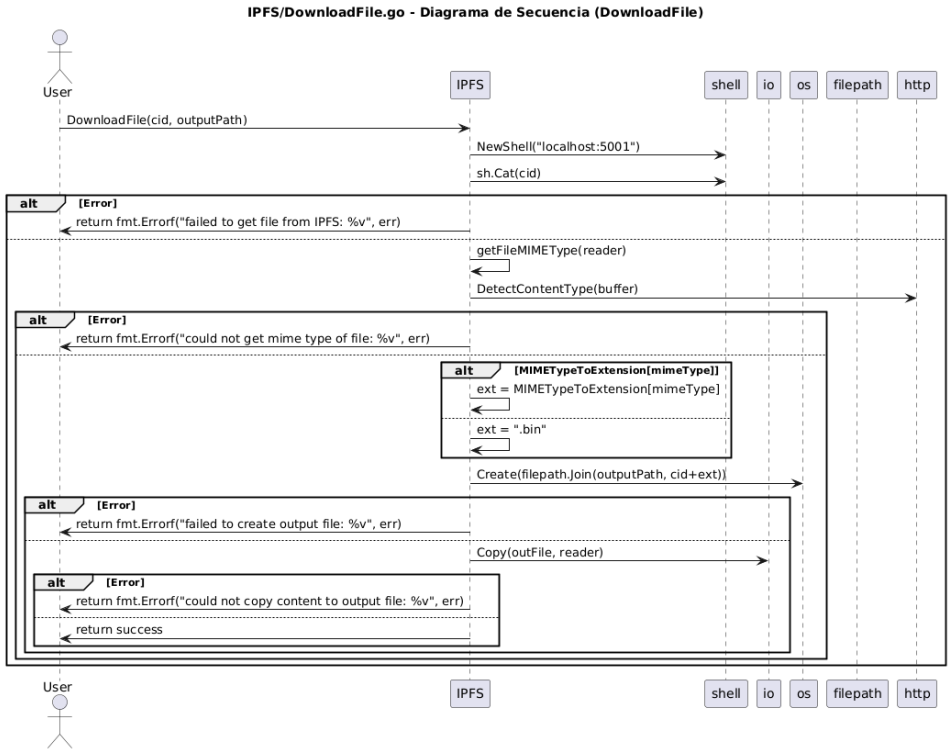
Anexos IX. Diagrama de clases función main-chaincode



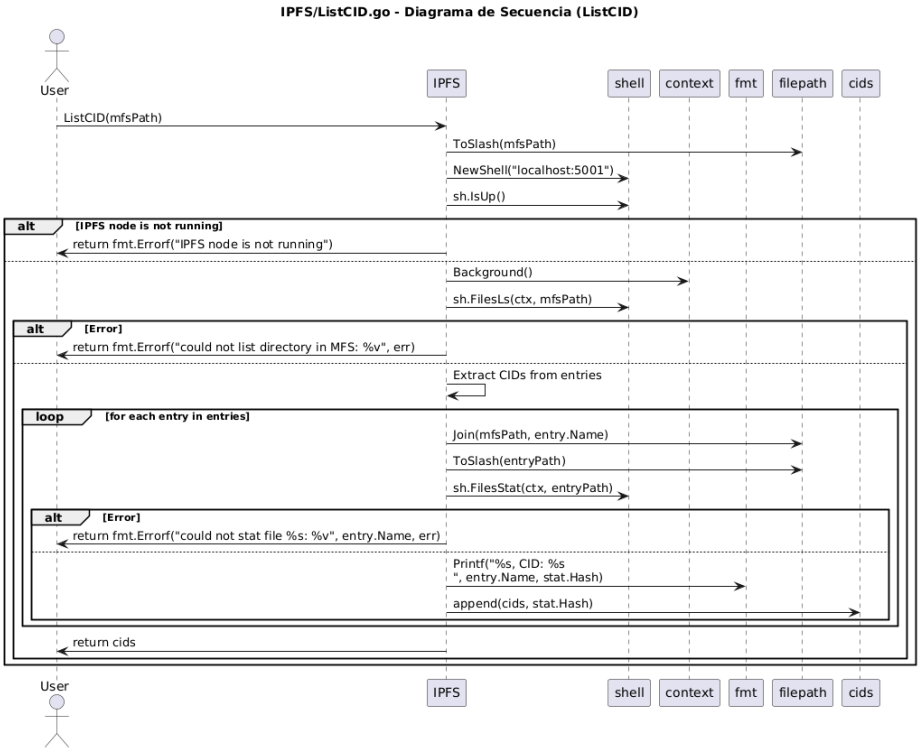
Anexos X. Diagrama de secuencia función IPFS GetFile



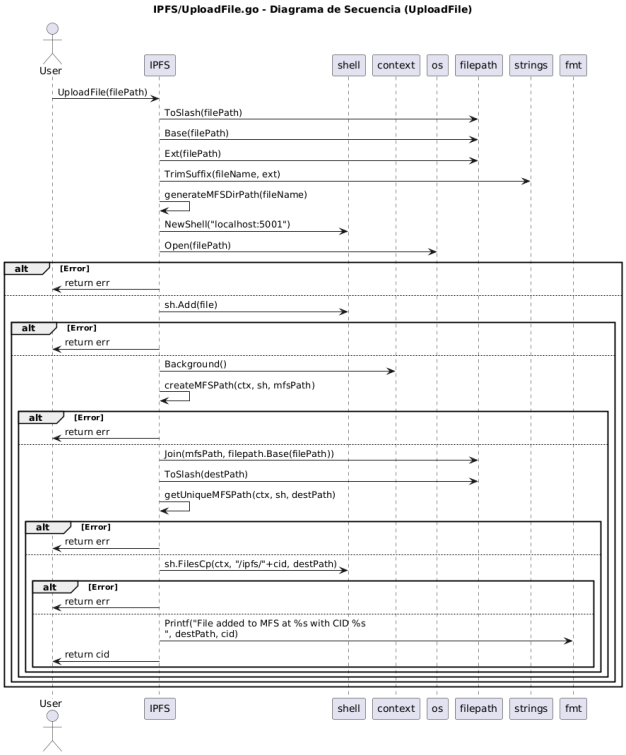
Anexos III. Diagrama de secuencia función IPFS DownloadFile



Anexos XI. Diagrama de secuencia función IPFS ListCID



Anexos XII. Diagrama de secuencia función IPFS UploadFile



ANEXO XIII. [Repositorio del prototipo]