PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS DE INFORMACIÓN

Trabajo de Titulación

Desarrollo de un prototipo de sistema de votación electrónica basado en blockchain

AUTOR:

Mao Nicolas Astudillo Andrade

DIRECTOR:

Henry Nelson Roa Marin, PhD.

QUITO DM, ABRIL DE 2025

Tabla de contenido

Índice De Ilustraciones

CAPÍTULO I – DEFINICIóN DEL PROYECTO DE TITULACIóN

1.1. Justificación

A nivel mundial, los sistemas de votación enfrentan desafíos relacionados con la seguridad y la transparencia, lo que ha impulsado el interés en soluciones tecnológicas como blockchain para mejorar la integridad electoral (Schilling & Wernicke, 2023). En Ecuador, aunque el sistema de votación sigue siendo mayormente manual, la modernización es necesaria para enfrentar problemas como fraudes y costos elevados (Singh et al., 2023).

En este contexto, el prototipo propuesto busca demostrar cómo la tecnología de blockchain puede mejorar la confiabilidad y transparencia en los procesos electorales, sentando las bases para su futura implementación en el país. Blockchain garantiza la inmutabilidad de los registros, lo que significa que los votos emitidos no podrán ser alterados o eliminados una vez registrados (Spanos & Kantzavelou, 2023). Al ser una red descentralizada, elimina la posibilidad de control o manipulación por parte de un solo actor, lo que asegura que cada voto sea contabilizado de manera transparente y verificable (Hjálmarsson et al., 2018). Esta capacidad de auditoría abierta, sumada a la seguridad criptográfica inherente a blockchain, mejora significativamente la confianza del votante en el proceso electoral.

La factibilidad del proyecto es alta, dado el desarrollo de plataformas blockchain como Solana, que proporcionan las herramientas necesarias para crear sistemas seguros y escalables (Solana Documentation, 2025). El objetivo no es implementar un sistema completo para una elección real, sino desarrollar un prototipo funcional que demuestre el potencial de blockchain. Esto hace que el proyecto sea realizable dentro del marco de

los recursos académicos disponibles y permite visualizar su aplicabilidad a gran escala en un futuro cercano.

1.2. Planteamiento del Problema

La integridad electoral se enfrenta a desafíos significativos en todo el mundo, y Ecuador no es la excepción. El sistema de votación actual, basado principalmente en procesos manuales, expone al país a problemas como la manipulación de resultados, desconfianza en los resultados y la falta de transparencia (Schilling & Wernicke, 2023). Estos factores socavan la legitimidad de los procesos electorales y perjudica la participación ciudadana.

El problema principal radica en la incapacidad del sistema electoral tradicional para garantizar un proceso confiable y demostrable a través de auditorías que no conlleven una gran cantidad de gastos y tiempo. Esto se traduce en altos costos operativos y en una percepción generalizada de desconfianza en el electorado.

Además, existen limitaciones tecnológicas y un bajo conocimiento de innovaciones como blockchain en el ámbito electoral, lo que dificulta aún más la implementación de un sistema moderno, seguro y transparente (Singh et al., 2023).

Ante esta situación, surge la interrogante central: ¿Cómo puede un sistema de votación electrónica genérico basado en tecnología blockchain contribuir a mejorar la seguridad, transparencia y confiabilidad del proceso electoral en Ecuador? Este planteamiento orienta la investigación hacia el desarrollo de un prototipo que demuestre el potencial de la tecnología blockchain para resolver estos problemas.

1.3. Objetivos

1.3.1. Objetivo General

1. Desarrollo de un prototipo de sistema de votación electrónica basado en blockchain.

1.3.2. Objetivo Específico

1. Analizar los requisitos funcionales y de seguridad necesarios en un sistema de votación electrónica en el contexto electoral ecuatoriano.
2. Seleccionar una plataforma blockchain adecuada para el diseño del prototipo.
3. Implementar el prototipo e incorporar un módulo de auditoría abierta que permita visualizar los resultados de las campañas.
4. Validar la funcionalidad del prototipo a través de una prueba controlada.

1.4. Alcance

El proyecto de titulación finalizará con el desarrollo de un prototipo funcional de un sistema de votación electrónica basado en blockchain, orientado a demostrar el potencial de esta tecnología para futuras aplicaciones. El sistema se enfocará en un funcionamiento básico, pero estructurado, e incluirá:

- Una interfaz para el registro de campañas y emisión de votos.
- Control de usuarios mediante el uso de billeteras digitales.
- Almacenamiento de los votos emitidos en una red de prueba blockchain.
- Validación de la consistencia de los votos a través de pruebas unitarias aplicadas al contrato inteligente, asegurando la creación de campañas validas, la unicidad del voto y la autenticidad del voto.
- Módulo de auditoría abierta, en el que los resultados pueden verificarse públicamente con relación a la dirección de billetera utilizada, sin revelar por cual opción voto cada votante.

Este proyecto no abarca los siguientes aspectos, por considerarse fuera del alcance técnico y temporal:

- Escalabilidad para elecciones nacionales.
- Implementación de mecanismos avanzados de autenticación o verificación ciudadana.
- Ciberseguridad aplicada a redes, dispositivos o sistemas externos a la blockchain.
- Aceptación social o legal del sistema de votación por parte de la ciudadanía o instituciones oficiales.

CAPÍTULO II – Marco Teórico

2.1. Sistemas de votación electrónica: enfoques, características y problemas

La votación electrónica se refiere al uso de dispositivos electrónicos o sistemas informáticos para emitir y contar votos, en contraste con el voto tradicional en papel. Existen múltiples enfoques actuales, desde máquinas de votación DRE (Direct Recording Electronic) en recintos electorales, hasta sistemas de escaneo óptico de boletas y plataformas de voto por Internet para sufragar remotamente. Cada enfoque busca mejorar la eficiencia del proceso electoral, pero también debe cumplir con requisitos estrictos de integridad y confianza.

2.1.1. Características Deseables

Diversos estudios académicos coinciden en las propiedades fundamentales que un sistema de votación electrónica debe garantizar. Según Haris et al. (2021), un sistema de e-voto eficiente debe asegurar seguridad (protección contra manipulación y accesos no autorizados), verificabilidad de los resultados, transparencia del proceso, privacidad del votante, accesibilidad para todos los ciudadanos (incluyendo personas con discapacidad o votantes remotos), así como precisión, rapidez en el escrutinio, objetividad, costo-efectividad y sostenibilidad. Entre estas propiedades, la literatura destaca especialmente la seguridad (garantizar que los votos no sean alterados ni revelados indebidamente), la verificabilidad de extremo a extremo (permitir auditorías independientes y que los votantes puedan confirmar que su voto fue contabilizado correctamente) y la accesibilidad (facilitar la participación de votantes geográficamente distantes o con impedimentos físicos) como pilares para mantener la confianza pública

en elecciones electrónicas. Un sistema óptimo debería proporcionar un balance entre estas características.

2.1.2. Enfoques Actuales y sus Retos

A lo largo de las últimas décadas se han implementado distintos sistemas de votación electrónica con resultados mixtos. Algunos países emplearon máquinas DRE con registro electrónico de votos, mientras que otros han experimentado con voto por Internet para población expatriada o fuerzas armadas. Estas innovaciones han traído beneficios como la agilización del escrutinio y la reducción de errores humanos, pero también han introducido nuevas preocupaciones. Un problema ampliamente documentado es la vulnerabilidad a ataques cibernéticos: investigadores han demostrado que fallas de software o medidas de seguridad insuficientes pueden permitir la alteración de votos a gran escala sin detección inmediata. De hecho, ciertas implementaciones fueron revertidas o limitadas debido a informes de inseguridad. Por ejemplo, Francia canceló el voto por Internet para sus electores en el extranjero en 2017 tras el dictamen de su agencia nacional de ciberseguridad (ANSSI) que lo consideró insuficientemente seguro. De igual modo, países como Alemania, Reino Unido, España o México se han mostrado reticentes a adoptar el voto electrónico remoto, citando la falta de mecanismos de auditoría robusta y riesgos para la integridad electoral. Querejeta-Azurmendi et al. (2020) señalan que en la votación remota por Internet el votante emite su sufragio en un entorno no controlado (p. ej., desde su hogar), lo que aumenta la posibilidad de coacción o compra de votos, así como el riesgo de suplantación de identidad o malware en el dispositivo del votante. Estas diferencias con respecto al entorno supervisado de una urna tradicional hacen que la seguridad de la votación en línea sea particularmente desafiante.

Adicionalmente, se han identificado problemas de transparencia y confianza en algunos sistemas electrónicos. El principio democrático exige que el proceso de votación sea comprensible y auditable por observadores independientes; sin embargo, cuando el conteo ocurre dentro de una máquina o programa opaco, el público puede desconfiar del resultado. La resistencia a fallos y la disponibilidad son otras preocupaciones: un error de software generalizado o un ataque de denegación de servicio podría afectar a muchos votantes simultáneamente en una elección electrónica, algo menos probable en el sistema tradicional.

En síntesis, los sistemas de votación electrónica actuales ofrecen ventajas de velocidad, eficiencia y potencial accesibilidad, pero enfrentan desafíos importantes. Los problemas conocidos incluyen vulnerabilidades técnicas que podrían comprometer resultados, dificultades para auditar de forma independiente los procesos, riesgos a la privacidad del votante y amenazas de coerción en entornos remotos. Estos retos han motivado abundante investigación académica para mejorar la confiabilidad de las elecciones electrónicas. Dentro de estas investigaciones recientes, se ha propuesto la tecnología blockchain como una posible solución para reforzar la seguridad y transparencia de los sistemas de votación, tal como se discute en las siguientes secciones.

2.2. Blockchain: fundamentos teóricos, propiedades y aplicaciones más allá de las criptomonedas

La tecnología blockchain (o cadena de bloques) surgió como la innovación fundamental detrás de la criptomoneda Bitcoin en 2008. En esencia, una blockchain es un libro mayor distribuido que agrupa transacciones u otros datos en bloques enlazados criptográficamente en secuencia temporal. Cada bloque contiene un hash criptográfico del bloque anterior, formando una cadena inmutable de registros. Los participantes de la

red mantienen múltiples copias sincronizadas de esta cadena y se ponen de acuerdo sobre su contenido mediante protocolos de consenso distribuido (como Prueba de Trabajo o Prueba de Participación), eliminando la necesidad de una autoridad central que valide las transacciones. Gracias a estas características, una blockchain correctamente implementada ofrece un alto grado de resistencia a la manipulación: una vez que un bloque de transacciones es confirmado por la red, resulta extremadamente difícil para un atacante alterarlo en todos los nodos sin ser detectado.

Entre las propiedades teóricas más destacadas de blockchain se encuentran la descentralización, inmutabilidad, transparencia y seguridad mediante criptografía. La descentralización implica que ninguna entidad única controla la cadena; el control se reparte entre muchos nodos iguales, lo que mejora la robustez frente a fallos o manipulaciones maliciosas en un solo punto. La inmutabilidad se refiere a la imposibilidad práctica de borrar o modificar registros ya confirmados: cualquier intento de alterar un bloque anterior invalidaría todos los bloques subsiguientes por el encadenamiento hash, haciendo evidente la alteración. Esta característica asegura, por ejemplo, que los votos almacenados en una blockchain no puedan ser cambiados después de emitidos. La transparencia significa que todos los nodos (y potencialmente el público, en cadenas abiertas) pueden inspeccionar las transacciones registradas, lo cual aumenta la trazabilidad y auditabilidad de la información; sin embargo, transparencia no equivale a revelación de identidad: en la mayoría de blockchains públicas, los usuarios operan con direcciones pseudónimas, aportando cierto grado de anonimato básico a nivel de identidad. Finalmente, la seguridad se apoya en algoritmos criptográficos: firmas digitales que garantizan la autenticidad de las transacciones y funciones hash que encadenan los bloques, combinados con mecanismos de consenso

que previenen que actores maliciosos tomen el control sin poseer la mayoría de la potencia de cómputo o participación en la red.

Además de sus bases teóricas, la blockchain se ha estudiado ampliamente por sus aplicaciones prácticas más allá de las criptomonedas. Inicialmente concebida para transferir valor (Bitcoin), pronto se reconoció que su modelo de registro fiable y distribuido podía transformar procesos en diversos dominios. Por ejemplo, en las finanzas, blockchain permite activos digitales y pagos entre pares sin intermediarios bancarios. En la gestión de cadenas de suministro, se utiliza para el seguimiento de productos, aportando proveniencia y trazabilidad desde el origen hasta el consumidor. Otras aplicaciones investigadas incluyen el Internet de las Cosas (coordinando redes de dispositivos con confianza), la gestión descentralizada de energía (redes eléctricas inteligentes P2P), los contratos inteligentes autoejecutables (Szabo, 1997) y, de especial relevancia para esta tesis, los sistemas de votación electrónica. De hecho, la votación es frecuentemente citada como un caso donde las propiedades de inmutabilidad y transparencia de blockchain podrían solventar problemas de integridad y confianza en elecciones digitales.

2.3. Smart contracts y plataformas blockchain (Ethereum vs. Solana)

Un componente clave de la evolución de blockchain más allá de las transacciones financieras es el smart contract o contrato inteligente. Nick Szabo acuñó el término en la década de 1990 para describir protocolos computacionales que ejecutarían automáticamente los términos de un contrato. Desde una perspectiva técnica moderna, un smart contract es esencialmente un programa autónomo almacenado y ejecutado en la blockchain, que se activa al cumplirse ciertas condiciones y puede imponer acuerdos entre partes sin necesidad de confiar en un intermediario. En otras

palabras, se trata de código que corre en la red descentralizada y cuyo estado (variables, saldos, etc.) es replicado en todos los nodos, garantizando que sus resultados sean consistentes y verificables por todos. Por ejemplo, un contrato inteligente podría representar las reglas de una elección (contabilizar votos, cerrar la votación a cierta hora, calcular ganadores) y la red blockchain se encargaría de ejecutar esas reglas tal como fueron programadas, sin posibilidad de intervención humana durante su ejecución.

2.3.1. Operación de los Contratos Inteligentes

La mayoría de las plataformas blockchain de segunda generación (como Ethereum) incorporan una máquina virtual (Virtual Machine) capaz de ejecutar código arbitrario en cada nodo. Los contratos inteligentes se escriben en lenguajes de alto nivel (por ejemplo, Solidity o Vyper en Ethereum) y luego se compilan a bytecode para la máquina virtual de la cadena (la EVM, Ethereum Virtual Machine, en el caso de Ethereum). Cuando un usuario envía una transacción que invoca una función de un contrato, esa transacción es incluida en un bloque y reproducida por todos los nodos: cada nodo ejecuta el código del contrato paso a paso determinísticamente, obteniendo el mismo resultado, lo que conduce a actualizar el estado del contrato (p. ej., registrar un voto) de forma consistente en toda la red. Esta ejecución colectiva brinda transparencia y confianza: el contrato actuará exactamente según su programación, y cualquier intento de alterar su lógica o resultados sería rechazado por los demás nodos. Sin embargo, también implica que el código de los smart contracts debe ser escrito con sumo cuidado, ya que los errores o vulnerabilidades en él serán replicados por todos. De hecho, incidentes famosos como el ataque al contrato The DAO en 2016 (donde un fallo de reentrancia en Solidity permitió robar fondos del contrato) demostraron que bugs en

contratos inteligentes pueden tener consecuencias catastróficas en un entorno inmutable (Atzei et al., 2017).

2.3.2. Comparativa entre Ethereum y Solana

Ethereum, propuesta en 2013 por Vitalik Buterin, fue la primera plataforma blockchain ampliamente adoptada que soportó contratos inteligentes flexibles, convirtiéndose en la base de miles de aplicaciones descentralizadas (dApps). Solana, lanzada en 2017 por Anatoly Yakovenko, es una plataforma más reciente que también soporta contratos inteligentes, pero con una arquitectura diferente, orientada a maximizar el rendimiento.

2.3.2.1. Rendimiento (throughput y latencia)

Ethereum tradicionalmente ha tenido un rendimiento limitado en su capa base, rondando 15 transacciones por segundo (TPS) debido a las restricciones de su mecanismo de consenso y al requisito de que cada nodo ejecute todas las transacciones. Esto ha llevado a congestión y tarifas altas en momentos de demanda elevada. Solana emplea un mecanismo llamado Proof of History (PoH) combinado con Prueba de Participación, que permite ordenar las transacciones de manera eficiente antes de alcanzarse el consenso BFT (Byzantine Fault Tolerance). Gracias a ello, Solana puede procesar en el orden de 65 000 TPS, acercándose a niveles de throughput de redes de pagos como Visa, y produce bloques con tiempos de unas decenas de cientos de milisegundos, logrando finalizaciones de transacciones en 1–2 segundos (Wu et al., 2024).

2.3.2.2. Tarifas y costos de transacción

En Ethereum, registrar cada voto en la cadena podría costar del orden de dólares por voto en periodos de congestión. Solana, al tener un throughput mayor, mantiene las tarifas extremadamente bajas (por ejemplo, $0.00025 USD por transacción en 2023), lo cual resulta crítico para un sistema electoral nacional (Wu et al., 2024).

2.3.2.3. Lenguajes de programación y entorno de ejecución

Ethereum utiliza Solidity y Vyper, que se ejecutan en la EVM, mientras que Solana adopta Rust (así como C/C++) como lenguaje principal para sus contratos, compilando a SBF (Solana Bytecode Format) para un runtime basado en LLVM. Rust, por diseño, evita problemas de memoria (p. ej., buffer overflows), lo que ofrece una base más segura frente a ciertos errores comunes en Solidity (Peterson et al., 2022).

2.3.2.4. Arquitectura y modelo de ejecución

Ethereum emplea un modelo monolítico donde todos los nodos ejecutan todas las transacciones. Solana permite ejecución paralela de transacciones que operen sobre cuentas distintas, lo que mejora significativamente el rendimiento. Además, Ethereum migró a PoS en 2022 (Ethereum 2.0) y usa soluciones de segunda capa (rollups, sharding futuro) para escalar, mientras que Solana escaló en capa base con PoH+PoS y Tower BFT.

2.3.2.5. Descentralización

Ethereum cuenta con cientos de miles de validadores tras su transición a PoS, lo que favorece la distribución global. Solana, con 1 000–2 000 validadores activos, ha sido objeto de críticas por una centralización relativa debida a sus elevados requisitos de hardware (Saleh, 2021).

2.3.2.6. Seguridad y fiabilidad de la red

Ethereum ha sufrido hacks a contratos (The DAO, Parity), lo que impulsó herramientas de análisis estático y buenas prácticas de programación (Atzei et al., 2017). Solana ha tenido interrupciones de red y vulnerabilidades en proyectos y en su modelo de cuentas, mostrando que ambas redes presentan riesgos que deben mitigarse con auditorías y testing riguroso (Wu et al., 2024).

2.3.3. Elección de Solana para el Prototipo

Solana ofrece la escalabilidad necesaria para manejar una elección con potencialmente millones de votos: su alto throughput y baja latencia permiten registrar votos casi en tiempo real sin congestionar la red. Además, sus tarifas bajas hacen viable un prototipo on-chain, y el modelo Rust/SBF aporta garantías de seguridad de memoria. Aunque Ethereum cuenta con un ecosistema más maduro, Solana facilita centrarse en la lógica de votación sin incurrir en elevados costos de gas. En consecuencia, Solana se alinea con los requisitos de rendimiento, costos y seguridad para un sistema de voto electrónico a escala, siempre aplicando buenas prácticas de desarrollo aprendidas de ambas plataformas.

2.4. Seguridad, transparencia y auditoría en votaciones digitales basadas en blockchain

La adopción de blockchain en votaciones digitales promete abordar varias necesidades críticas: integridad electoral, anonimato del votante y resistencia a ataques. A continuación, se evalúan estas promesas según la literatura científica.

2.4.1. Integridad y seguridad del voto

Una de las mayores ventajas de blockchain es su capacidad de garantizar la integridad de los registros. Cada voto registrado como transacción en una blockchain pública queda inmutable y vinculado criptográficamente a los demás, de modo que es prácticamente imposible alterar un voto ya emitido sin detección (Cortier et al., 2023). Esto proporciona protección contra fraude electoral basado en manipulación de actas o cambios posteriores al cierre de la votación. La ausencia de una autoridad central única dificulta ataques internos: ningún administrador solitario puede alterar unilateralmente los resultados, ya que sería necesario comprometer a la mayoría de los nodos de la red. Además, la arquitectura distribuida ofrece tolerancia a fallos bizantinos; por ejemplo, mientras no se supere el umbral de nodos maliciosos (p. ej., 1/3 en BFT o 51 % en PoW/PoS), la red sigue operativa.

2.4.2. Disponibilidad y resistencia a ataques de denegación de servicio

Una infraestructura de voto centralizada puede sufrir ataques DDoS, impidiendo la votación. En cambio, en una blockchain pública robusta, no existe un único punto de falla, la red peer-to-peer en su conjunto tendría que ser atacada, algo mucho más complejo. Incluso si algunos nodos caen, otros mantienen la operatividad.

2.4.3. Transparencia y auditoría

Blockchain proporciona un nivel de transparencia sin precedentes. Toda transacción (voto) queda publicada en el libro mayor distribuido, permitiendo a cualquier observador descargar la cadena y verificar de forma independiente el conteo (Cortier et al., 2023). La verificabilidad end-to-end se logra al entregar a cada votante un recibo criptográfico (hash) que le permite confirmar que su voto fue incluido correctamente; además, cualquier tercero puede realizar un reconteo universal. Esto

elimina gran parte de la dependencia de la fe en las autoridades electorales y simplifica la auditoría por observadores independientes.

2.4.4. Privacidad y anonimato del votante

Mantener el secreto del voto en una plataforma transparente requiere técnicas criptográficas adicionales. Esquemas con cifrado homomórfico, firmas ciegas, mixnets o pruebas de conocimiento cero disocian identidad y voto. Por ejemplo, protocolos como Fujioka-Okamoto-Ohta (1992) usan firmas ciegas para garantizar que el administrador firme la boleta sin conocer su contenido, y luego se publica el voto cifrado contabilizable sin revelar al votante. Otros, como Open Vote Network, implementan pruebas de cero conocimiento para privacidad total y auto-escrutinio (McCorry et al., 2017). Para resistencia a coacción, se proponen mecanismos de re-votación y votos señuelo (dummy), como en NetVote (Querejeta-Azurmendi et al., 2020), permitiendo que un votante anule un voto forzado sin que el coercitor pueda distinguirlo.

2.4.5. Resistencia a ataques y robustez

Blockchain dificulta manipulaciones internas y censura de votos: incluso si un nodo malicioso intenta excluir transacciones, otros validadores honestos las procesarán. La redundancia global asegura que los datos persisten aunque algunos nodos se corrompan. Sin embargo, expertos como Park et al. (2020) advierten que blockchain no mitiga riesgos en el dispositivo del votante (malware, phishing) ni elimina complejidad que podría introducir nuevas superficies de ataque (contratos vulnerables). Por tanto, blockchain es una parte de un diseño integral de seguridad que debe considerar también autenticación, usabilidad y protección del cliente.

En síntesis, blockchain puede reforzar la integridad, transparencia y disponibilidad de las elecciones, pero requiere técnicas criptográficas para proteger la privacidad y un diseño global que aborde el eslabón más débil: el dispositivo del votante.

2.5. Estudios previos y soluciones similares de voto electrónico con blockchain

El campo de voto electrónico basado en blockchain ha florecido con numerosos prototipos y propuestas académicas. A continuación, se revisan algunos proyectos representativos:

2.5.1. EtherVote

Sistema totalmente descentralizado en Ethereum donde registro de votantes, emisión y conteo residen en smart contracts. Busca transparencia e inmutabilidad, pero enfrenta desafíos de costo de gas y escalabilidad en comicios de gran tamaño (Spanos & Kantzavelou, 2023).

2.5.2. Open Vote Network (OVN)

Contrato inteligente en Ethereum para elecciones de pequeño grupo (≤ 60 votantes), self-tallying y privacidad total mediante pruebas de cero conocimiento. Limitado por costos crecientes y vulnerabilidades a ataques de ordenamiento de transacciones por mineros (McCorry et al., 2017).

2.5.3. NetVote

Esquema centrado en resistencia estricta a la coerción y re-votación con votos dummy aleatorios. Utiliza credenciales anónimas temporales y pruebas de cero conocimiento para verificar votos sin revelar identidad, mejorando usabilidad al no requerir claves previas (Querejeta-Azurmendi et al., 2020).

2.5.4. Voatz: aplicación móvil empleada en elecciones en West Virginia (2018)

Con backend blockchain. Auditoría del MIT encontró vulnerabilidades que permitían interceptar o modificar boletas, subrayando la necesidad de rigurosas evaluaciones de seguridad (MIT, 2020).

CAPÍTULO III – DESARROLLO DEL PROTOTIPO

3.1. Enfoque metodológico y técnico

Para el desarrollo del prototipo se optó por una metodología de cascada, estructurada en fases secuenciales (requisitos, diseño, implementación, verificación y mantenimiento), lo que permitió validar de forma rigurosa cada componente antes de avanzar a la siguiente etapa y garantizar la calidad del sistema en un entorno controlado.

Desde el punto de vista técnico, la arquitectura se diseñó sobre diversos componentes, justificando la elección de cada uno en función de sus fortalezas:

3.1.1. Blockchain Solana (Devnet)

Se seleccionó Solana por su elevada capacidad de procesamiento de transacciones y baja latencia, características esenciales para asegurar la escalabilidad de la plataforma durante las pruebas de concepto (Solana Labs, 2023).

3.1.2. Framework Anchor (Rust)

Anchor simplifica enormemente la escritura, las pruebas y el despliegue de programas en Solana al proporcionar plantillas, macros de seguridad y mecanismos de validación de cuentas en tiempo de compilación, lo cual reduce la complejidad del código y mitiga posibles vulnerabilidades en contratos inteligentes (Anchor Labs, 2023).

3.1.3. Supabase (PostgreSQL off-chain)

Se adoptó Supabase como backend para el almacenamiento de información off-chain por varias razones: su compatibilidad nativa con PostgreSQL, la facilidad de implementación de un backend completo en cuestión de minutos mediante su consola visual y CLI, y la familiaridad previa del desarrollador con la plataforma. Además, su sistema de Row Level Security (RLS) permite definir políticas de acceso a nivel de fila directamente desde la base de datos, reforzando el control de permisos desde el frontend (Supabase Inc., 2023).

3.1.4. Next.js (React) en frontend

La elección de Next.js responde a su capacidad para ofrecer rendering híbrido (SSR/SSG) y una arquitectura modular basada en componentes. Asimismo, el uso de archivos ".tsx" facilita la combinación de sintaxis HTML y TypeScript en un mismo fichero, mejorando la productividad y la detección temprana de errores de tipado durante el desarrollo (Vercel, 2023).

3.1.5. Node.js con Express como capa intermedia

Esta combinación brinda un entorno de ejecución eficiente y no bloqueante para implementar la API que orquesta las interacciones entre la blockchain y la base de datos. Además, Express se integra de forma nativa con la definición de interfaz de programas de Solana (Solana Interface Definition Language, IDL), lo cual automatiza la generación de clientes y simplifica las llamadas a los contratos inteligentes al partir de un esquema tipado (Node.js Foundation, 2023; Solana Labs, 2023).

3.1.6. Autenticación con Phantom y wallet-adapter

Para la gestión de identidades se integró la cartera Phantom mediante el paquete wallet-adapter de Solana, lo cual elimina la necesidad de credenciales tradicionales y ofrece una experiencia de usuario fluida y segura basada en estándares de Web3 (Solana Labs, 2023).

3.2. Análisis de requerimientos funcionales y no funcionales

3.2.1. Requerimientos funcionales

3.2.1.1. F1. Gestión de campañas

El sistema permite crear campañas de votación con título, descripción, opciones de voto y fechas de inicio y fin solo a administradores. Cada campaña creada genera un token (PDA) para identificar la campaña dentro de la blockchain. Adicionalmente, debe ser posible consultar las campañas públicas existentes por cualquier usuario.

3.2.1.2. F2. Registro y autorización de votantes

Debe existir un mecanismo para registrar votantes autorizados en cada campaña. Sólo un administrador podrá registrar como votante un usuario en una campaña al momento de creación de esta, lo cual se reflejará en una tabla relacional (voter_campaign en la base de datos). Al registrarse un votante, el sistema emite (mint) un token NFT de voto único asociado a ese votante y a esa campaña, que representa su derecho a votar.

3.2.1.3. F3. Emisión de voto

El sistema garantiza que cada votante emita exactamente un voto por campaña. Para lograrlo, el votante debe poseer un NFT válido (emitido en F2) y, al momento de votar, dicho token es quemado (burn) en la blockchain, eliminándolo de circulación. Esto asegura la unicidad del voto: una vez utilizado el token, el votante no puede volver a votar en la misma campaña.

3.2.1.4. F4. Sincronización y almacenamiento de resultados

Los resultados de la votación (conteo de votos por opción) deben sincronizarse periódicamente desde la blockchain hacia la base de datos para su persistencia y consulta eficiente. Específicamente, el sistema extrae el conteo de votos on-chain de cada campaña (atributo campaign.votes en el contrato inteligente) en intervalos regulares y guarda snapshots de estos conteos en una tabla vote_result_indexed, junto con una marca temporal (recorded_at). Esto permite mantener un histórico de la evolución de votos a lo largo del tiempo.

3.2.1.5. F5. Auditoría pública

Se requiere un módulo de auditoría accesible públicamente (sin autenticación) que muestre la evolución histórica de los votos por opción para cualquier campaña. Cualquier usuario, aunque no esté registrado ni autenticado, podrá consultar las campañas finalizadas o en curso y visualizar, de forma gráfica e interactiva, cómo han avanzado los resultados.

3.2.2. Requerimientos no funcionales

3.2.2.1. Seguridad y privacidad

Se enfatizó la protección de la integridad del proceso de votación y de los datos personales. Solo un administrador autenticado puede crear una campaña y asignar votantes a esta. Adicionalmente, se implementaron políticas de seguridad a nivel de base de datos utilizando Row Level Security (RLS) de PostgreSQL (a través de Supabase). Estas políticas RLS aseguraron que cada votante (identificado por su wallet) solo pudiera insertar o actualizar su propia relación voter_campaign y ningún otro dato.

3.2.2.2. Escalabilidad y rendimiento

En la blockchain Solana (Devnet), el contrato inteligente fue desarrollado con Anchor optimizando el uso de cuentas y operaciones. Se utilizaron Program Derived Addresses (PDA) para las cuentas de campaña, lo que permite generar direcciones de cuenta de manera determinística a partir de combinaciones de seeds y la clave del programa, evitando colisiones o duplicados en la creación de cuentas de datos. Así mismo, para almacenar los votos se usaron contadores dentro de la cuenta de la campaña, evitando tener que crear una transacción por cada voto para persistencia individual.

3.2.2.3. Usabilidad

Se priorizó la experiencia de usuario para que el sistema fuera intuitivo a pesar de la complejidad subyacente de blockchain. El front-end, construido con Next.js, ofreció una interfaz moderna y unificada: los votantes se autenticaron únicamente mediante su cartera Phantom (integración vía wallet-adapter, sin necesidad de registro tradicional con usuario/contraseña), eliminando fricciones de doble autenticación. La UI presenta un diseño moderno (tema oscuro) con navegación clara para realizar las tres acciones principales: registro en una campaña, emisión de voto y consulta de auditoría.

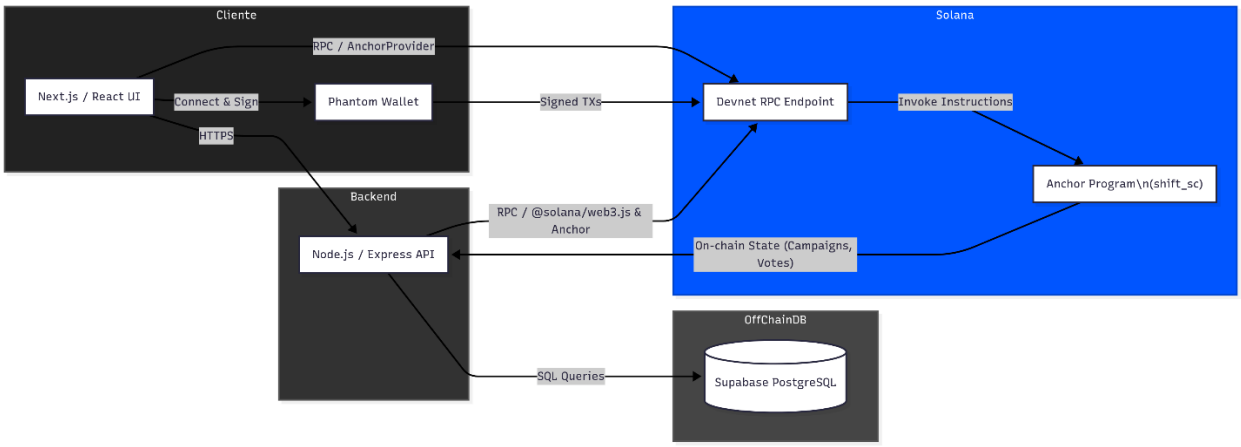
Se realizaron pruebas de uso informales para refinar la interfaz, asegurando que incluso usuarios no familiarizados con blockchain pudieran seguir el flujo (conectar wallet, votar) de forma clara.

3.3. Diseño del sistema

3.3.1. Arquitectura general

La arquitectura del sistema se diseñó en múltiples capas, integrando componentes off-chain (fuera de la cadena de bloques) y on-chain (dentro de la blockchain Solana) de manera coordinada. Esto es descrito en un diagrama de arquitectura (ver Ilustración 1).

Ilustración 1
Arquitectura general del sistema.



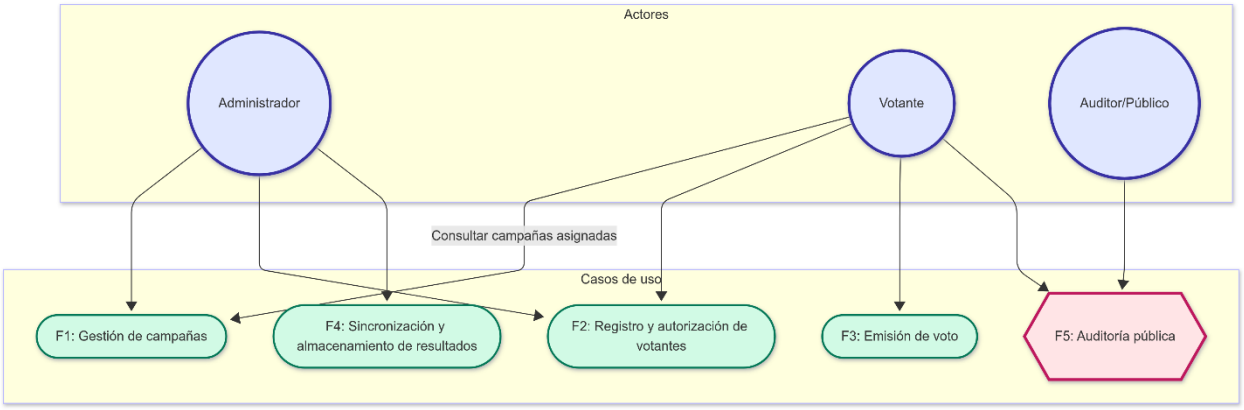
Nota. Diagrama de la arquitectura general del sistema.

La arquitectura sigue un patrón híbrido: la lógica crítica de voto se mantiene en la blockchain para garantizar transparencia e inmutabilidad, mientras que las funcionalidades complementarias (gestión de usuarios, persistencia de históricos, interfaz gráfica) residen off-chain para aprovechar herramientas convencionales de desarrollo web.

3.3.2. Casos de uso

Se identificaron tres roles principales en el sistema, cuyas interacciones se modelaron en un diagrama de casos de uso (ver Ilustración 2).

Ilustración 2
Diagrama de casos de uso.



Nota. Diagrama de casos de uso del sistema.

3.3.2.1. Administrador

Usuario con privilegios para gestionar campañas: tras autenticarse en Supabase (wallet registrada como administrador), crea campañas de votación, define título, descripción, opciones, fechas y wallets autorizadas. Al crear la campaña, también inicia el mint del NFT que servirá para generar los NFTs de voto.

3.3.2.2. Votante

Participante en una o varias campañas: conecta su wallet Phantom, y consulta las campañas a las que ha sido asignado. Durante el periodo activo emite su voto; esto quema su NFT y registra la elección on-chain y off-chain. Solo puede votar una vez por campaña.

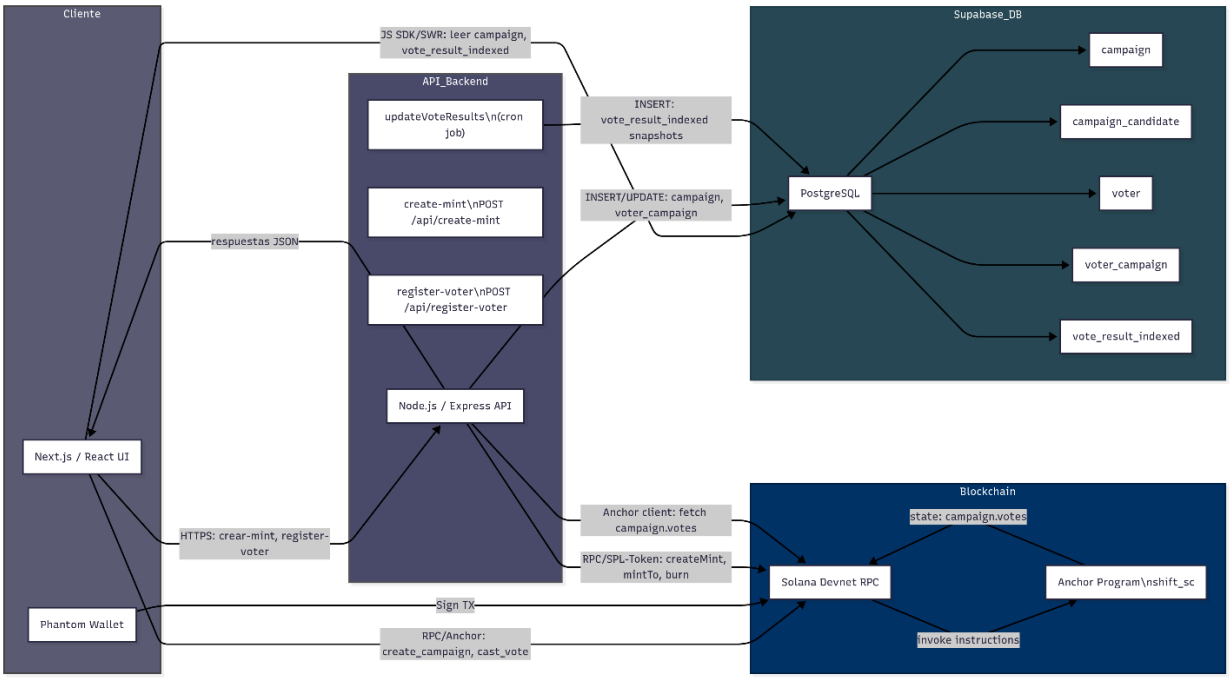
3.3.2.3. Auditor/Público

Cualquier usuario externo: accede al módulo de auditoría pública, selecciona una campaña y observa la evolución de votos en tiempo real, sin credenciales y sin capacidad de modificación; su función es garantizar la transparencia antes y después de la elección.

3.3.3. Componentes y flujo de datos

La solución se compone de cuatro componentes principales, cuyos roles e interacciones se describen a continuación (ver Ilustración 3):

Ilustración 3
Diagrama de flujo de datos.



Nota. Diagrama de flujo de datos del sistema.

3.3.3.1. Front-end (Next.js + React) – Interfaz web

Conecta la wallet Phantom mediante supabase-auth-helpers (JWT) sin login adicional. Incluye páginas /admin/new (crear campañas), /vote (emitir votos) y /audit (auditoría pública). Valida reglas básicas en el cliente y usa Anchor/solana-web3 para enviar transacciones y consultar la blockchain; sincroniza resultados a través de la API o librerías de Supabase.

3.3.3.2. API Backend (Node.js + Express) – Intermediario seguro

Expone rutas REST críticas (p. ej., /api/register-voter, /api/create-mint). Registra votantes, genera mints SPL de campaña y ejecuta on-chain el mint/burn de NFTs. Un cron job cada 60 segundos lee el estado de votos en la blockchain y guarda instantáneas en vote_result_indexed, manteniendo histórico y actualización frecuente.

3.3.3.3. Contrato inteligente (Solana + Anchor) – Núcleo lógico

Escrito en Rust, define cuentas PDA de Campaña con metadatos y contador de votos. Instrucciones create_campaign y cast_vote validan parámetros, registran el mint SPL, exigen un NFT válido, queman el token al votar y actualizan contadores. Anchor aporta la IDL y verificaciones de cuentas, simplificando la interacción cliente-cadena.

3.3.3.4. Base de datos (Supabase PostgreSQL) – Almacenamiento off-chain

Tablas admin_wallet, campaign, candidate, campaign_candidate, voter, voter_campaign y vote_result_indexed. Políticas RLS protegen datos (p. ej., voter_campaign sólo permite inserciones al propio wallet). Guarda históricos de

resultados, mapea usuarios con wallets y permite cotejar la información con registros on-chain para trazabilidad completa.

3.4. Desarrollo del prototipo

(Ver Anexo 1 para esquema de base datos)

3.4.1. Contrato inteligente (Solana + Anchor)

Desarrollado en Rust: define la cuenta Campaña con tamaño fijo y valida hasta un número máximo de opciones. Cada campaña crea su propio Mint SPL-Token que sirve de "comprobante" de voto; a cada votante se le emite uno y la instrucción cast_vote lo quema mediante CPI (Cross-Program Invocation) al Token Program, garantizando unicidad y reflejando los votos pendientes. Probado en localnet, luego desplegado en Devnet; Anchor generó la IDL para luego ser integrada tanto en front-end como en backend.

3.4.2. Interfaz de usuario (Next.js + React)

SPA que integra el wallet adapter de Phantom; al conectarse, verifica/crea el perfil en Supabase. Muestra campañas abiertas, invoca POST /api/register-voter para registrar y mintear el NFT, y usa el cliente Anchor para firmar la transacción cast_vote. Tras confirmación, la UI marca al usuario como "votó". Página /audit renderiza gráficos (Recharts/Chart.js) con snapshots de vote_result_indexed, sin exponer datos sensibles (ver Anexo 2 para capturas de pantalla de la interfaz).

3.4.3. Módulo de auditoría abierta

Sección pública sin autenticación que consulta los históricos de resultados cada minuto desde Supabase y muestra líneas/barras por opción, porcentajes y metadatos

(inicio, fin, participación). No revela la opción del votante, pero muestra si ha votado o no.

3.5. Integración con blockchain (Solana Devnet)

3.5.1. Despliegue en Solana Devnet

El contrato se lanzó en la red de pruebas pública usando SOL de airdrop; Anchor generó la IDL que consumen front-end y back-end para llamadas tipadas al programa.

3.5.2. Direcciones determinísticas (PDAs y ATAs)

Cada campaña ocupa una PDA (Program Derived Address) derivada de la semilla fija “campaign” + creador + identificador, evitando colisiones. Los NFTs de voto se guardan en la ATA (Associated Token Account) del votante (derivada de su clave + mint de campaña) hasta ser quemados.

3.5.3. Proceso de votación (cast_vote)

El front-end prepara la transacción Anchor con las cuentas: PDA de campaña, ATA y mint del votante, Token Program y firmante. Phantom solicita la firma, se envía a Devnet y la confirmación se detecta vía confirmTransaction.

3.5.4. Sincronización de resultados

Se prefirió polling cada 60 s sobre listeners WebSocket: el backend lee los contadores de la cuenta de campaña y guarda un snapshot en vote_result_indexed. El

método resultó simple, fiable y de baja carga para el prototipo, dejando abierta la opción de optimizar en producción.

3.6. Pruebas y validación

3.6.1. Pruebas unitarias del contrato (Anchor + Mocha/Chai)

Se cubrieron casos de error y "happy path" para create_campaign (mínimo de opciones, fechas válidas, colisión de PDA) y cast_vote (periodo inválido, opción inexistente, falta de NFT, mint incorrecto, doble voto, concurrencia). Se verificó que los códigos de error personalizados aparezcan y que, en escenarios válidos, el token NFT se queme y los contadores on-chain se incrementen correctamente (ver Anexo 3 para resultados de pruebas del Smart-contract).

3.6.2. Simulación de campaña en Devnet

Se lanzó una campaña real "Destino Vacaciones 2025" (Mompiche, Punta Sal, Casa Blanca) con amigos como votantes Phantom. El sistema mintió un NFT a cada wallet, los participantes votaron sin complicaciones y los tokens se quemaron al instante. Los contadores on-chain, los snapshots del backend y el recuento manual coincidieron, confirmando UX fluida y lógica correcta (ver Anexo 4 para capturas de pantalla de la creación, voto y gráficos de auditoría de la campaña mencionada).

3.6.3. Validación de unicidad y consistencia

La combinación de restricciones en voter_campaign y quema de NFT en el contrato garantizó un solo voto por participante. El backend almacena snapshots

acumulativos monótonos, evitando incoherencias; los totales finales coincidieron con la suma de snapshots y con el número de NFTs emitidos menos quemados. Se demostró así que el prototipo ofrece votación única, íntegra, transparente y auditable.

CAPÍTULO IV – RESULTADOS Y VALIDACIÓN

4.1. Resultados obtenidos en las pruebas

El sistema de votación electrónica basado en blockchain fue sometido a pruebas unitarias, de integración y simulaciones con usuarios para verificar su correcto funcionamiento. En las pruebas unitarias, cada componente del smart contract y de la aplicación fue evaluado por separado; se confirmó que las funciones de registro y conteo de votos operaban según lo esperado, impidiendo votos duplicados o no autorizados. Posteriormente, las pruebas de integración validaron el flujo completo del proceso: un votante emitía su voto a través de la interfaz, este voto era cifrado y enviado a la blockchain de Solana, y finalmente se reflejaba en el conteo almacenado en la cadena. Durante las simulaciones con usuarios, se observó que la interfaz permitía emitir votos de manera intuitiva y que cada usuario recibía confirmación inmediata de la recepción de su sufragio, evidenciando una experiencia de voto satisfactoria y sin errores en la contabilización.

Los resultados cualitativos de estas pruebas demostraron el comportamiento correcto del sistema en escenarios controlados. En particular, el prototipo logró mitigar intentos de fraude (p. ej., impidiendo la duplicación de votos) y garantizó que cada voto registrado permaneciera inmutable y accesible para auditoría en la cadena de bloques. Asimismo, el sistema ofreció opciones de votación tanto remota (en línea) como presencial simulada, replicando condiciones de un entorno real y reduciendo la necesidad de desplazamiento físico de los votantes, lo cual es un beneficio señalado en la literatura. En conjunto, las pruebas confirmaron que el prototipo cumple con los

requisitos funcionales básicos: cada voto válido es registrado sin poder ser borrado o editado, sin alteraciones posteriores, y el conteo final refleja fielmente los votos emitidos.

4.2. Análisis de desempeño del prototipo

En cuanto a la carga sobre la red y uso de almacenamiento, el diseño del prototipo se enfocó en la eficiencia. Cada voto genera una transacción mínima que sólo actualiza un vector de contadores Vec<u64> alojado en la cuenta de campaña permitiendo de manera teórica una cantidad de votos infinita. El prototipo fijó **10 opciones** por campaña para la prueba, aunque la arquitectura admite **más de 200** sin cambios sustanciales. Al guardar únicamente los conteos acumulados (no los votos individuales), la huella on-chain se mantiene reducida y la escritura no satura la red. Las pruebas confirmaron que, con este límite y estructura, el uso de almacenamiento se mantuvo dentro de rangos manejables y el sistema conserva capacidad de escalar con degradación mínima, siempre que se optimice el manejo de datos en cadena.

4.3. Limitaciones del prototipo desarrollado

4.3.1. Escalabilidad

Aunque Solana ofrece gran rendimiento, cualquier cadena pública puede enfrentar cuellos de botella si el volumen sube a escala nacional. En futuros ciclos se podrá optimizar la distribución de carga dentro y fuera de la blockchain, pues la aplicación web sería la más vulnerable a este tipo de escenarios donde el padrón electoral crece.

4.3.2. Seguridad y resiliencia

El prototipo ya incorpora buenas prácticas, pero aún no pasa por auditorías formales ni pruebas de penetración masivas. Siguientes iteraciones deberían incluir revisión de contratos por terceros y mecanismos de recuperación ante ataques de red o fallos de infraestructura.

4.3.3. Validación de identidad

En el prototipo solo se registra una wallet de forma simplificada. De cara a un despliegue en producción, se prevé integrar identidades digitales soberanas, credenciales verificables y autenticación biométrica para asegurar que cada ciudadano vote exactamente una vez. Estas mejoras también permitirán prevenir fraudes adicionales, por ejemplo, confirmar que el votante siga con vida o aplicar inhabilitaciones legales por antecedentes penales o deudas

4.3.4. Brecha digital

El diseño actual presupone que todos los electores cuentan con conexión a internet y saben manejar una wallet, un supuesto poco realista para comicios a gran escala. Las próximas versiones deberán incorporar métodos de autenticación más intuitivos para el ciudadano y trasladar la custodia de las billeteras a una entidad estatal, de modo que la complejidad técnica recaiga en la infraestructura pública y no en el votante.

4.3.5. Privacidad del voto

El conteo agregado ya impide vincular votos a identidades, pero el anonimato pleno demanda criptografía más avanzada. Futuras iteraciones podrían adoptar cifrado

homomórfico y aplicar cifrado extremo a extremo en todas las comunicaciones, incluidas las peticiones web, de modo que un atacante interpuesto, incluso en redes domésticas o inseguras, no pueda interceptar información sensible ni deducir preferencias individuales.

4.3.6. Validación a gran escala

Hasta ahora, la plataforma solo se ha ensayado en laboratorio con un grupo reducido de usuarios. Las próximas fases deberían contemplar pilotos controlados con miles de votantes, simulaciones de estrés rigurosas y la verificación de compatibilidad con los sistemas electorales existentes, junto con estudios de aceptación social y adecuación al marco legal.

CAPÍTULO V – CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

El proyecto demostró satisfactoriamente la viabilidad de usar la blockchain de Solana para un sistema de votación electrónica seguro, transparente y auditable. El prototipo integró front-end, back-end, contrato inteligente y módulo de auditoría, asegurando la inmutabilidad de cada sufragio y una experiencia de usuario sencilla. Aun así, para su adopción en procesos electorales reales será necesario fortalecer la validación de identidad, incorporar técnicas criptográficas avanzadas de privacidad y validar la solución a gran escala dentro del marco legal vigente.

1. Se identificaron y documentaron con detalle los requisitos de autenticidad del votante, unicidad del sufragio, integridad de datos y transparencia, adaptados al contexto electoral ecuatoriano, y se tradujeron en reglas de negocio y controles criptográficos del contrato inteligente.
2. Tras comparar varias opciones, se eligió Solana por su alto rendimiento y bajas comisiones. Las pruebas confirmaron que su modelo de cuentas y PDAs se ajusta bien a campañas electorales con contadores inmutables.
3. Se desarrolló un prototipo completo que combina front-end, back-end, contrato Anchor y base de datos. El módulo de auditoría abierta ofrece visualizaciones en tiempo real sin exponer datos sensibles, reforzando la transparencia del proceso.
4. Una simulación con votantes reales en Devnet verificó la correcta emisión, quema y conteo de votos. Los resultados on-chain, los snapshots off-chain y el recuento manual coincidieron, evidenciando la solidez del flujo de registro, votación y auditoría.

5.2. Recomendaciones

Basado en la experiencia y conocimiento obtenido, y de las limitaciones identificadas, se proponen las siguientes líneas de mejora para evolucionar el prototipo de votación electrónica basado en blockchain:

1. Debe reforzarse la privacidad del sufragio mediante técnicas criptográficas avanzadas; la combinación de cifrado homomórfico con pruebas de conocimiento cero permitiría contar votos cifrados y certificar su validez sin revelar su contenido, preservando así el anonimato del elector mientras se mantiene la verificabilidad pública.
2. Resulta indispensable robustecer la validación de identidad ciudadana. Integrar credenciales gubernamentales, identidades digitales soberanas o biometría, e incluso la unión de varios factores de autenticación, garantizará que solo los ciudadanos habilitados voten y que cada persona lo haga una única vez, alineando el sistema con los estándares oficiales del padrón electoral.
3. Es prioritario blindar el sistema contra ciberataques mediante cifrado extremo a extremo en todas las comunicaciones, certificado pinning, monitoreo continuo de tráfico y mecanismos de detección y mitigación de intrusiones. A ello debe sumarse un proceso riguroso de pruebas de penetración y hardening de infraestructura para prevenir ataques de denegación de servicio o manipulación de datos, asegurando que la cadena de custodia de cada voto permanezca intacta desde el dispositivo del elector hasta la blockchain.

REFERENCIAS

Anchor Labs. (2023). Anchor: Solana development framework. https://www.anchor-lang.com

Cortier, V., Gaudry, P., Glondu, S., et al. (2023). Security of electronic voting: Vulnerabilities and solutions (INRIA Research Report). https://www.inria.fr/en/security-electronic-voting-digital-security-confidentiality

Ding, Y., Peng, H., & Li, X. (2025). A Comprehensive Study of Exploitable Patterns in Smart Contracts: From Vulnerability to Defense (arXiv:2504.21480). arXiv. https://arxiv.org/abs/2504.21480

Haris, A., et al. (2021). Electronic voting system: Nature, origin and its global application. International Journal of Innovation, Creativity and Change, 15(2), 1333-1350. https://www.researchgate.net/publication/388177939_Electronic_Voting_System_Nature_Origin_and_Its_Global_Application

Jafar, U., Ab Aziz, M. J., & Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. Electronics, 10(9), 1010. https://pmc.ncbi.nlm.nih.gov/articles/PMC8434614/

McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy (Open Vote Network). In International Conference on Financial Cryptography and Data Security. https://pmc.ncbi.nlm.nih.gov/articles/PMC8434614/

Node.js Foundation. (2023). Node.js. https://nodejs.org

Park, S., Specter, M., Narula, N., & Rivest, R. (2021). Going from bad to worse: From Internet voting to blockchain voting. Journal of Cybersecurity, 7(1), tyaa025. https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf

Querejeta-Azurmendi, I., Arroyo Guardeño, D., Hernández-Ardieta, J. L., & Hernández Encinas, L. (2020). NetVote: A strict-coercion resistance re-voting based Internet voting scheme with linear filtering. Mathematics, 8(9), 1618. https://www.mdpi.com/2227-7390/8/9/1618

Solana Labs. (2023). Wallet Adapter for Solana. https://github.com/solana-labs/wallet-adapter

Spanos, A., & Kantzavelou, I. (2023). EtherVote: A blockchain-based electronic voting system (arXiv:2307.10726). arXiv. https://arxiv.org/abs/2307.10726

Specter, M., Koppel, J., & Weitzner, D. J. (2020). Security analysis of Voatz, the first Internet voting application used in U.S. federal elections. In 29th USENIX Security Symposium. https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf

Supabase Inc. (2023). Supabase documentation. https://supabase.com

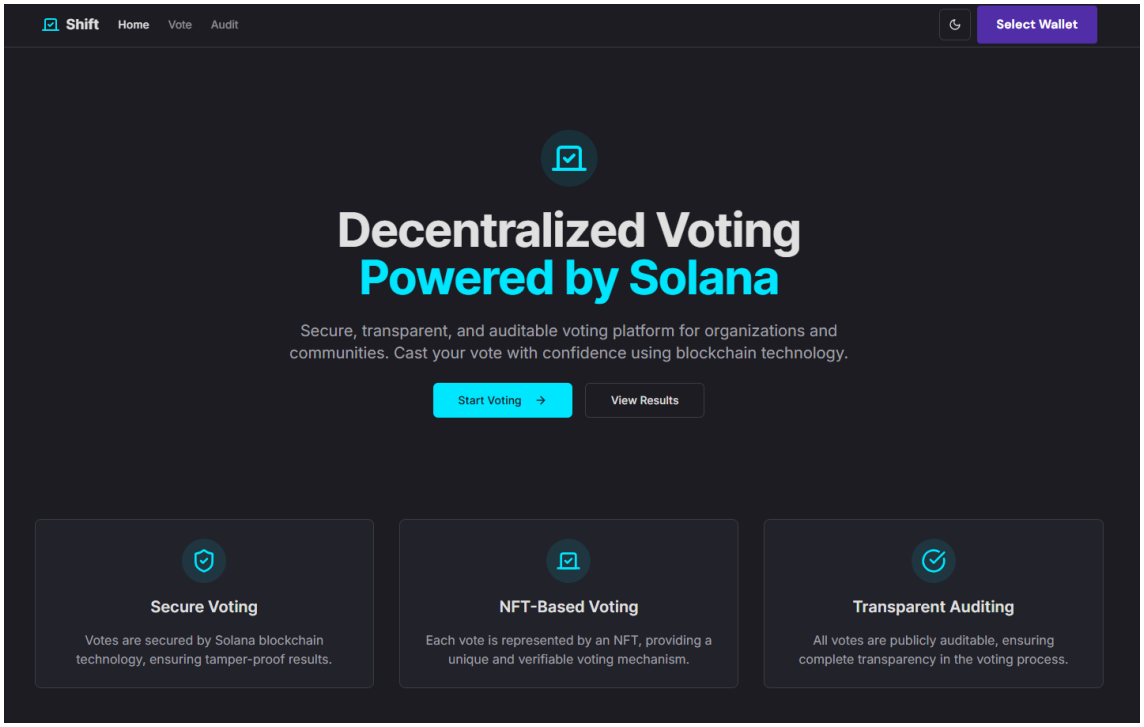
Vercel. (2023). Next.js. https://nextjs.org

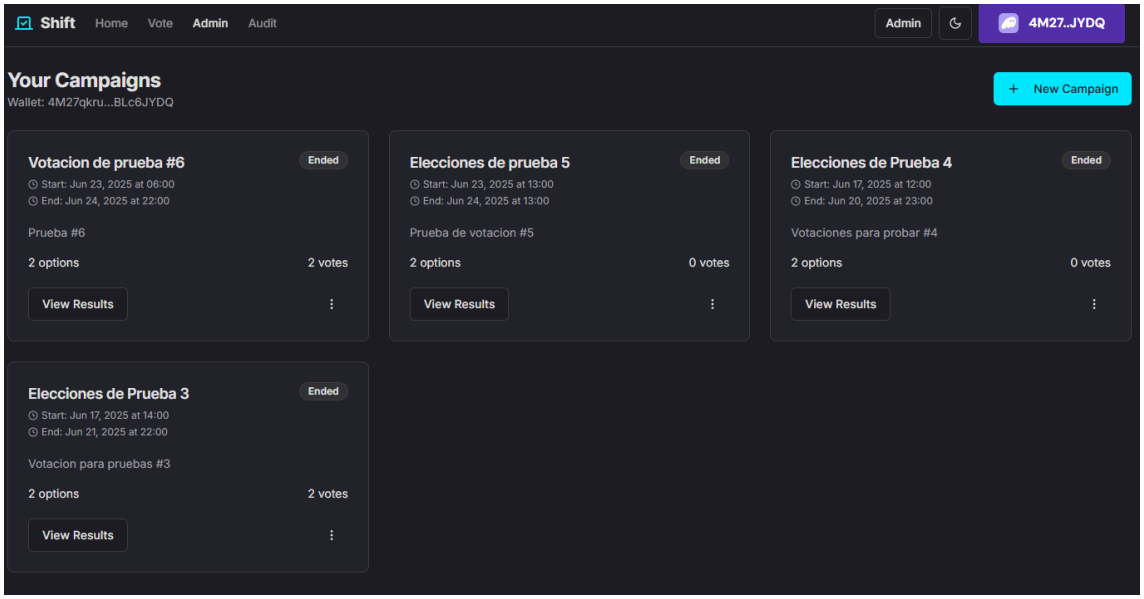
Wu, X., Xing, J., & Li, X. (2024). Exploring vulnerabilities and concerns in Solana smart contracts (arXiv:2504.07419). arXiv. https://arxiv.org/abs/2504.07419

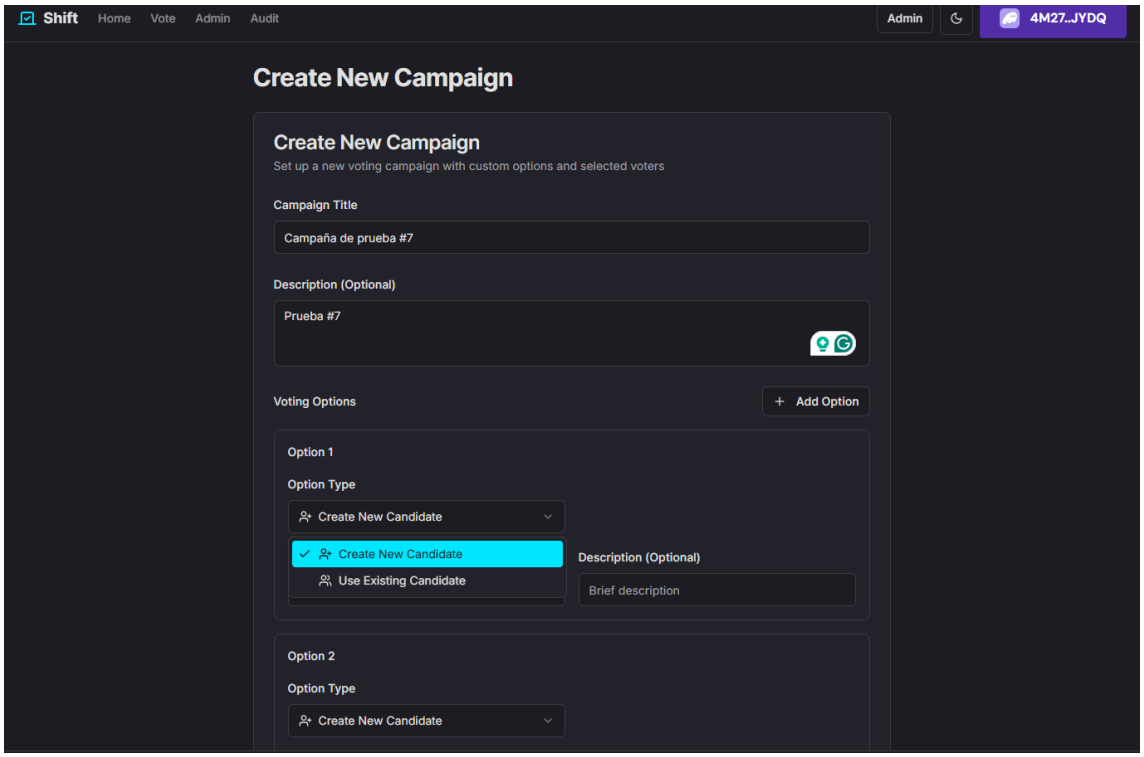
ANEXOS

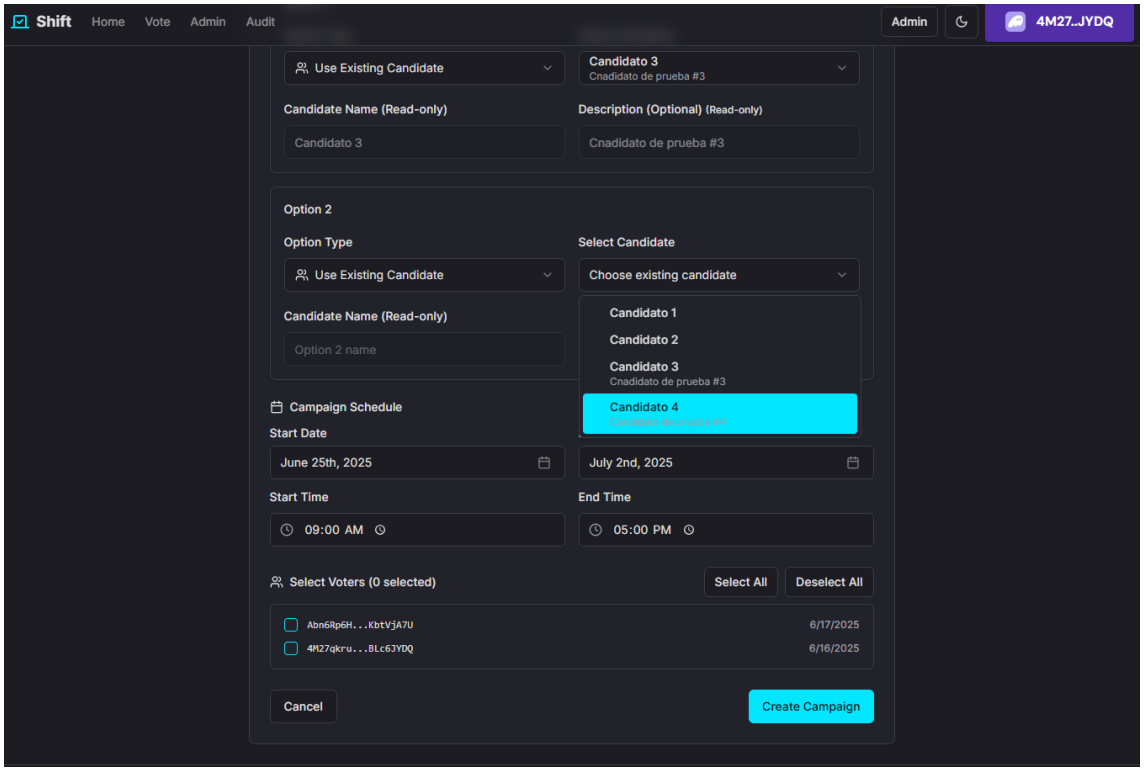
ANEXO 1. Esquema de base de datos Supabase

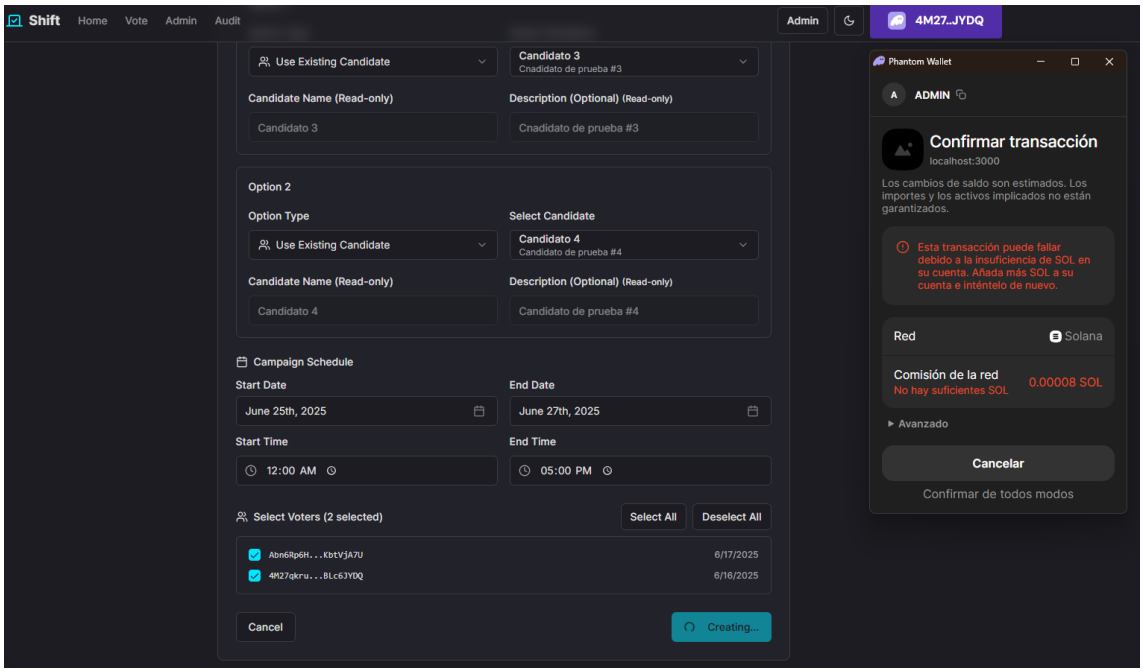
ANEXO 2. Capturas de pantalla Interfaz de Usuario

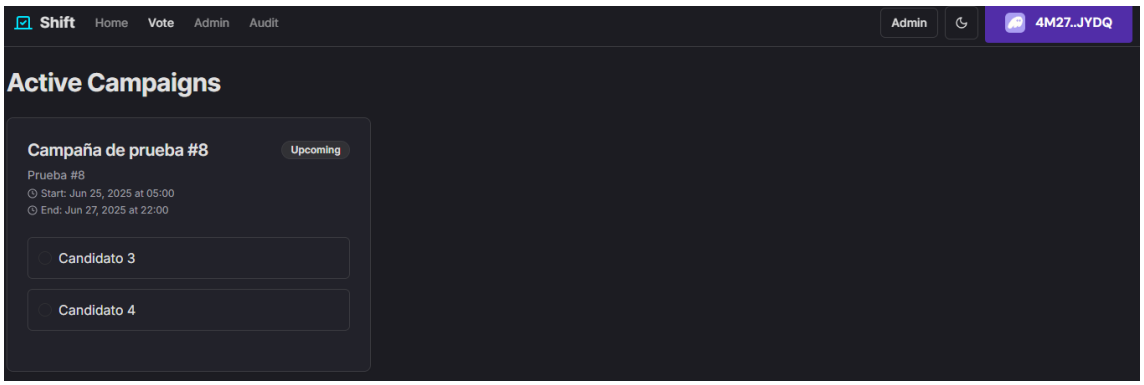


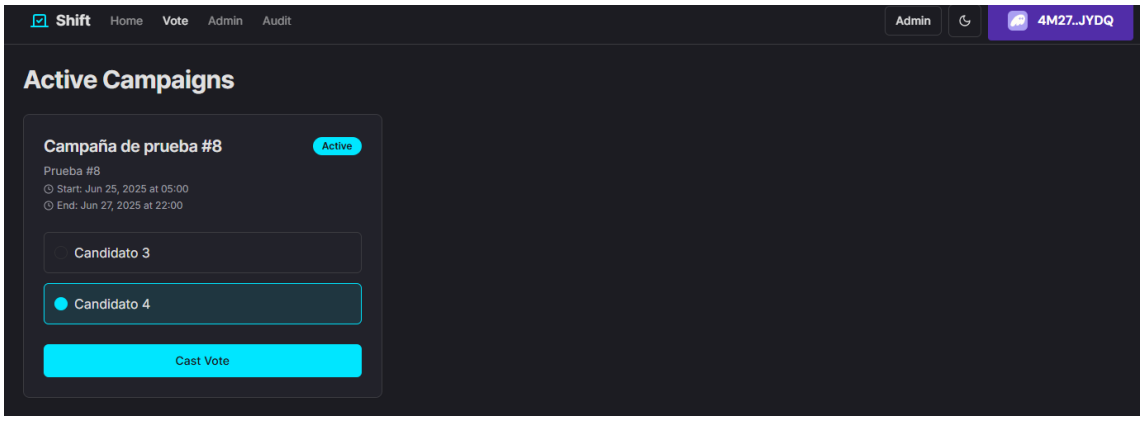


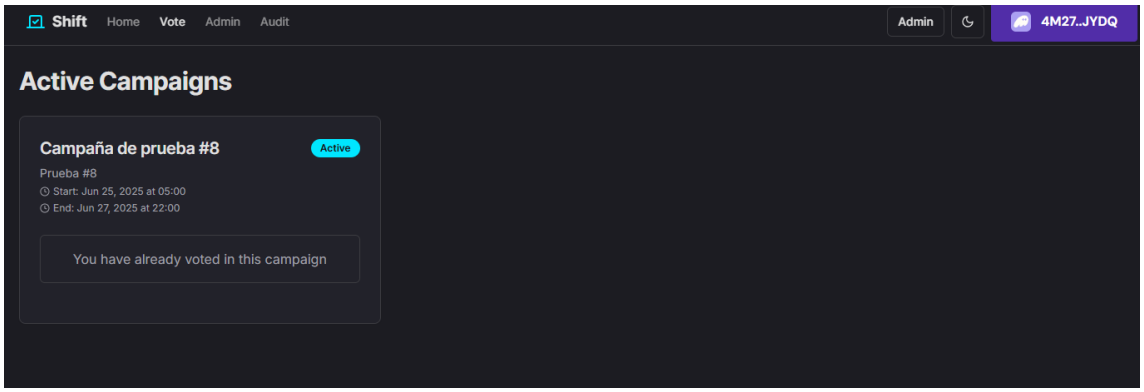

Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Create New Campaign
Create New Campaign
Set up a new voting campaign with custom options and selected voters
Campaign Title
Campaña de prueba #7
Description (Optional)
Prueba #7
Voting Options
Add Option
Option 1
Option Type
Create New Candidate
Create New Candidate
Use Existing Candidate
Description (Optional)
Brief description
Option 2
Option Type
Create New Candidate

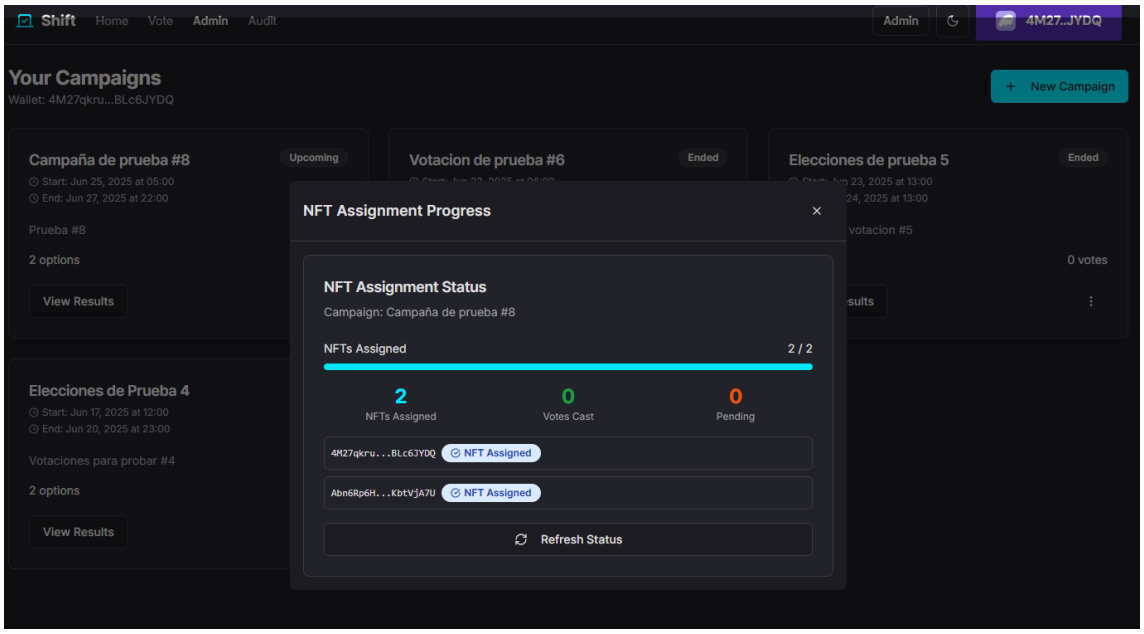

Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Use Existing Candidate
Candidato 3
Cnadidato de prueba #3
Candidate Name (Read-only)
Candidato 3
Description (Optional) (Read-only)
Cnadidato de prueba #3
Option 2
Option Type
Use Existing Candidate
Select Candidate
Choose existing candidate
Candidate Name (Read-only)
Option 2 name
Candidato 1
Candidato 2
Candidato 3
Cnadidato de prueba #3
Candidato 4
Campaign Schedule
Start Date
June 25th, 2025
July 2nd, 2025
Start Time
09:00 AM
End Time
05:00 PM
Select Voters (0 selected)
Select All
Deselect All
Abn6Rp6H...KbtVjA7U
6/17/2025
4M27qkru...BLc6JYDQ
6/16/2025
Cancel
Create Campaign

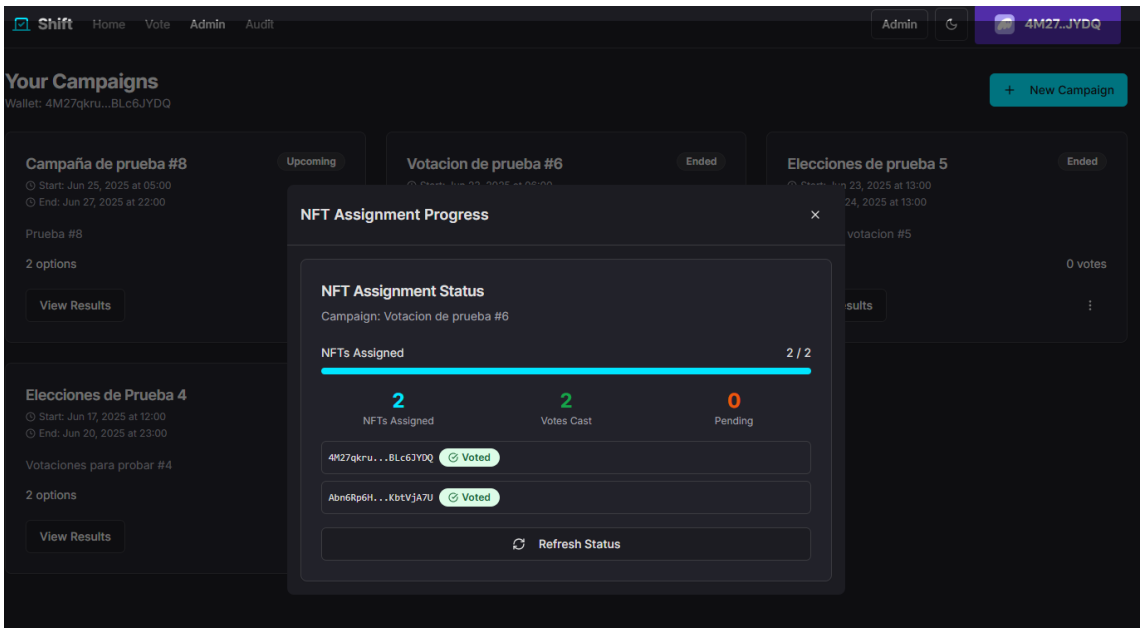

Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Use Existing Candidate
Candidato 3
Cnadidato de prueba #3
Candidate Name (Read-only)
Description (Optional) (Read-only)
Candidato 3
Cnadidato de prueba #3
Option 2
Option Type
Select Candidate
Use Existing Candidate
Candidato 4
Candidato de prueba #4
Candidate Name (Read-only)
Description (Optional) (Read-only)
Candidato 4
Candidato de prueba #4
Campaign Schedule
Start Date
End Date
June 25th, 2025
June 27th, 2025
Start Time
End Time
12:00 AM
05:00 PM
Select Voters (2 selected)
Select All
Deselect All
Abn6Rp6H...KbtVjA7U
6/17/2025
4M27qkru...BLc63YDQ
6/16/2025
Cancel
Creating...
Phantom Wallet
ADMIN
Confirmar transacción
localhost:3000
Los cambios de saldo son estimados. Los importes y los activos implicados no están garantizados.
Esta transacción puede fallar debido a la insuficiencia de SOL en su cuenta. Añada más SOL a su cuenta e inténtelo de nuevo.
Red
Solana
Comisión de la red
No hay suficientes SOL
0.00008 SOL
Avanzado
Cancelar
Confirmar de todos modos

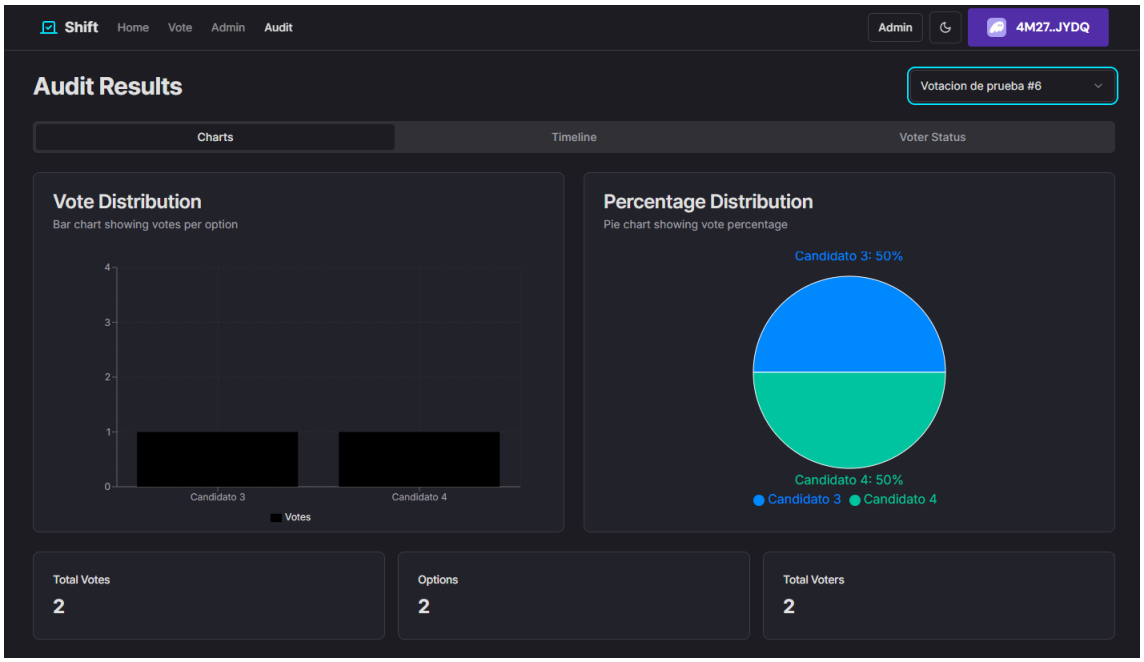

Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Active Campaigns
Campaña de prueba #8
Upcoming
Prueba #8
Start: Jun 25, 2025 at 05:00
End: Jun 27, 2025 at 22:00
Candidato 3
Candidato 4

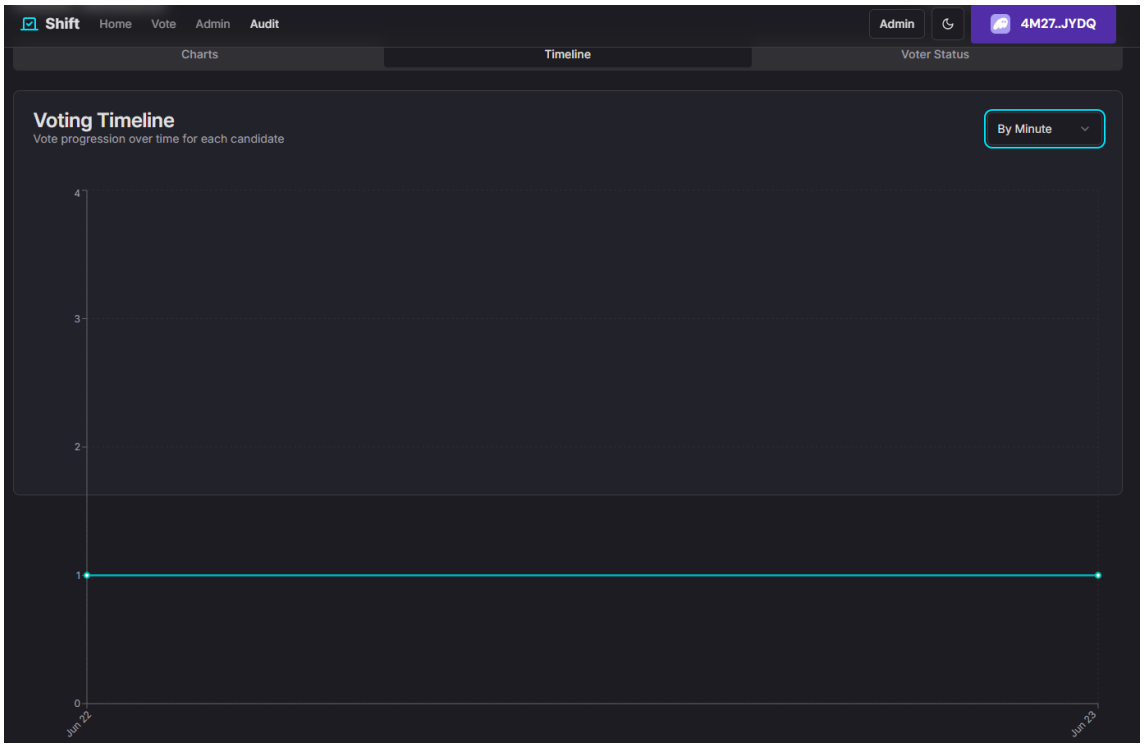

Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Active Campaigns
Campaña de prueba #8
Active
Prueba #8
Start: Jun 25, 2025 at 05:00
End: Jun 27, 2025 at 22:00
Candidato 3
Candidato 4
Cast Vote

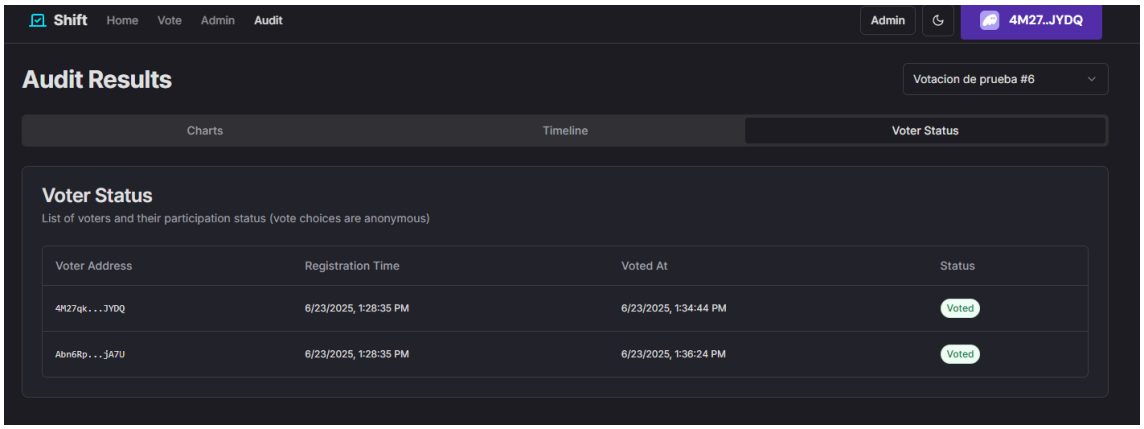

Shift
Home
Vote
Admin
Audit
Admin
4M27...JYDQ
Active Campaigns
Campaña de prueba #8
Active
Prueba #8
Start: Jun 25, 2025 at 05:00
End: Jun 27, 2025 at 22:00
You have already voted in this campaign


Shift
Home
Vote
Admin
Audit
Admin
4M27...JYDQ
Your Campaigns
Wallet: 4M27qkru...BLc6JYDQ
New Campaign
Campaña de prueba #8
Upcoming
Start: Jun 25, 2025 at 05:00
End: Jun 27, 2025 at 22:00
Prueba #8
2 options
View Results
Votacion de prueba #6
Ended
Elecciones de prueba 5
Ended
votacion #5
0 votes
Elecciones de Prueba 4
Start: Jun 17, 2025 at 12:00
End: Jun 20, 2025 at 23:00
Votaciones para probar #4
2 options
View Results
NFT Assignment Progress
NFT Assignment Status
Campaign: Campaña de prueba #8
NFTs Assigned
2 / 2
2
NFTs Assigned
0
Votes Cast
0
Pending
4M27qkru...BLc6JYDQ
NFT Assigned
Abn6Rp6H...KbtVjA7U
NFT Assigned
Refresh Status

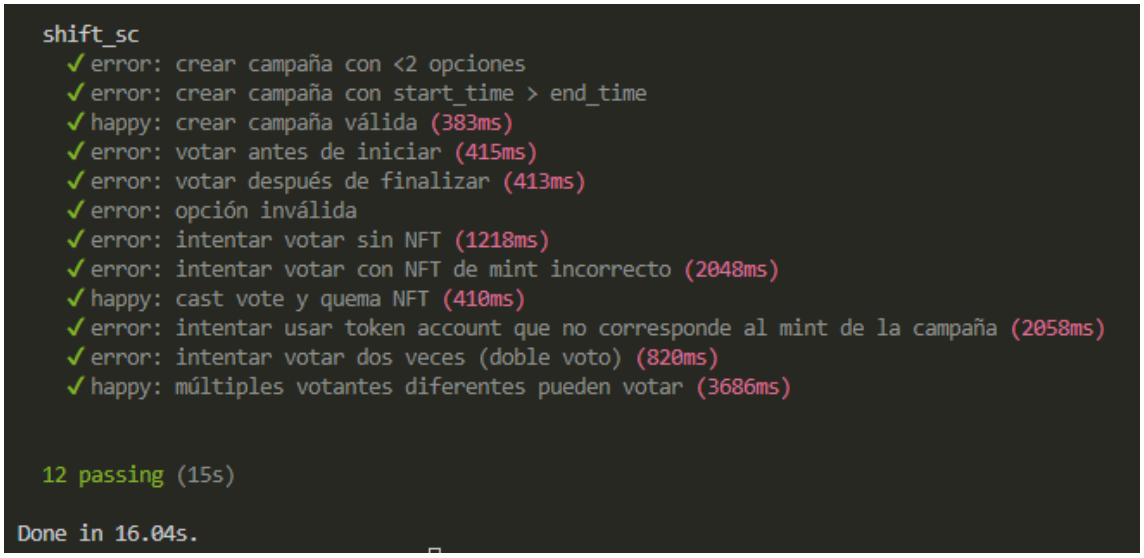

Shift
Home
Vote
Admin
Audit
Admin
4M27...JYDQ
Your Campaigns
Wallet: 4M27qkru...BLc6JYDQ
New Campaign
Campaña de prueba #8
Upcoming
Start: Jun 25, 2025 at 05:00
End: Jun 27, 2025 at 22:00
Prueba #8
2 options
View Results
Votacion de prueba #6
Ended
Elecciones de prueba 5
Ended
votacion #5
0 votes
Elecciones de Prueba 4
Start: Jun 17, 2025 at 12:00
End: Jun 20, 2025 at 23:00
Votaciones para probar #4
2 options
View Results
NFT Assignment Progress
NFT Assignment Status
Campaign: Votacion de prueba #6
NFTs Assigned
2 / 2
2
NFTs Assigned
2
Votes Cast
0
Pending
4M27qkru...BLc6JYDQ
Voted
Abn6Rp6H...KbtVjA7U
Voted
Refresh Status


Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Audit Results
Votacion de prueba #6
Charts
Timeline
Voter Status
Vote Distribution
Bar chart showing votes per option
4
3
2
1
0
Candidato 3
Candidato 4
Votes
Percentage Distribution
Pie chart showing vote percentage
Candidato 3: 50%
Candidato 4: 50%
Candidato 3
Candidato 4
Total Votes
2
Options
2
Total Voters
2

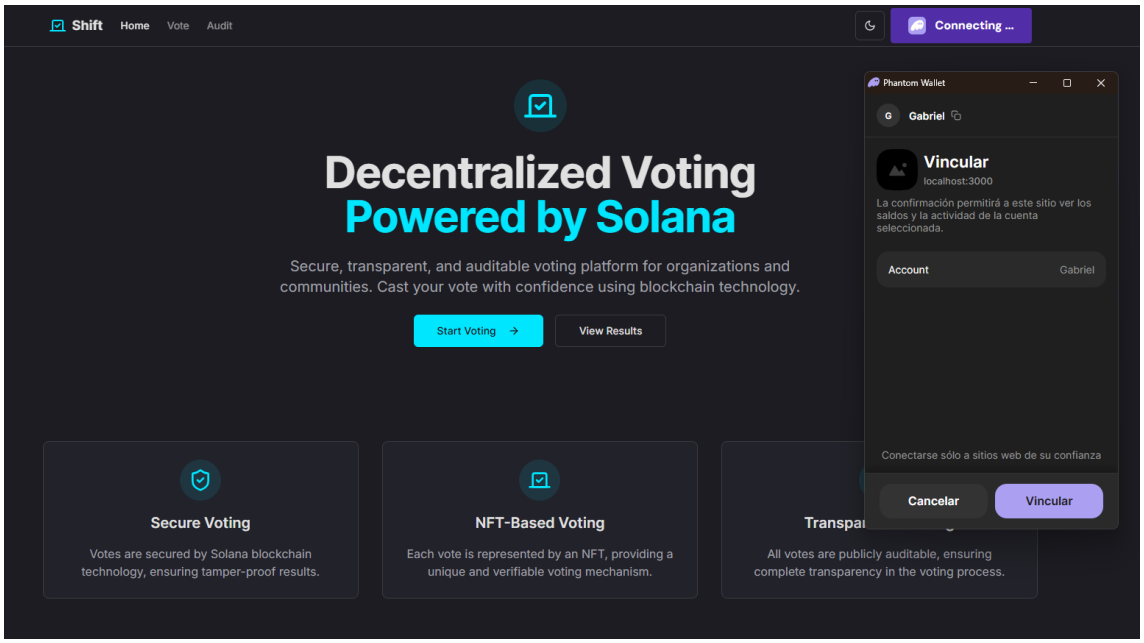

Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Charts
Timeline
Voter Status
Voting Timeline
Vote progression over time for each candidate
By Minute
4
3
2
1
0
Jun 22
Jun 23

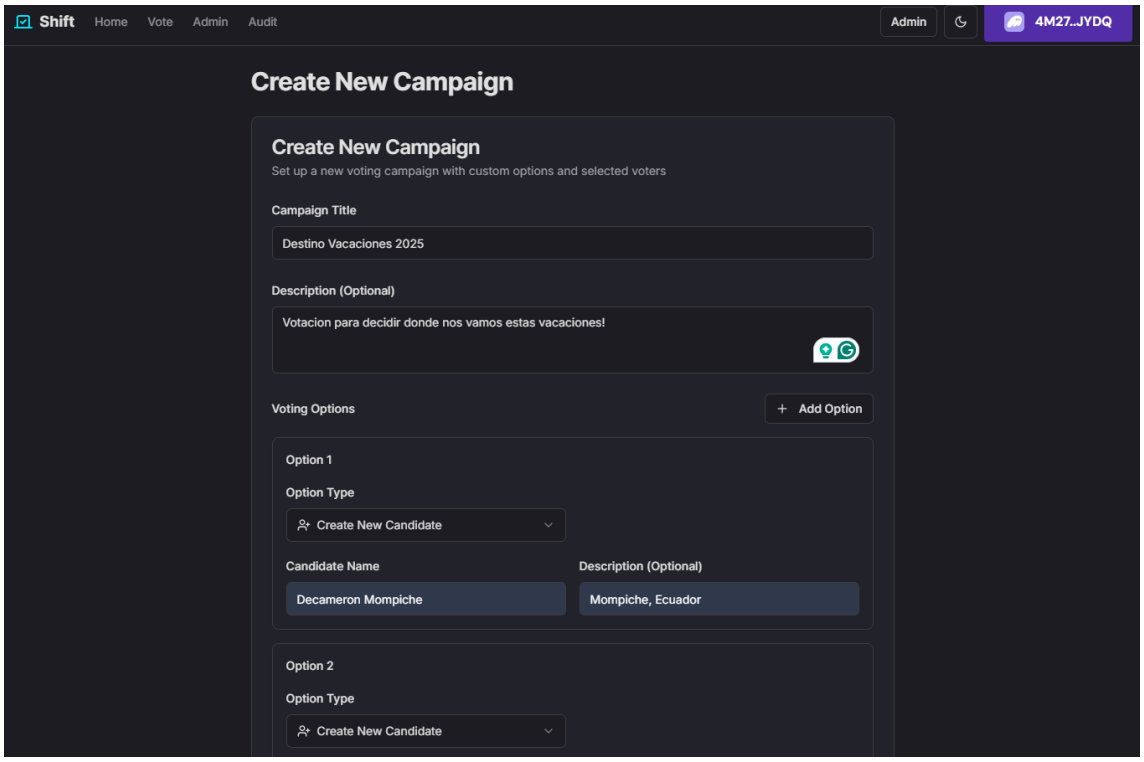

Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Audit Results
Votacion de prueba #6
Charts
Timeline
Voter Status
Voter Status
List of voters and their participation status (vote choices are anonymous)
Voter Address
Registration Time
Voted At
Status
4M27qk...JYDQ
6/23/2025, 1:28:35 PM
6/23/2025, 1:34:44 PM
Voted
Abn6Rp...jA7U
6/23/2025, 1:28:35 PM
6/23/2025, 1:36:24 PM
Voted

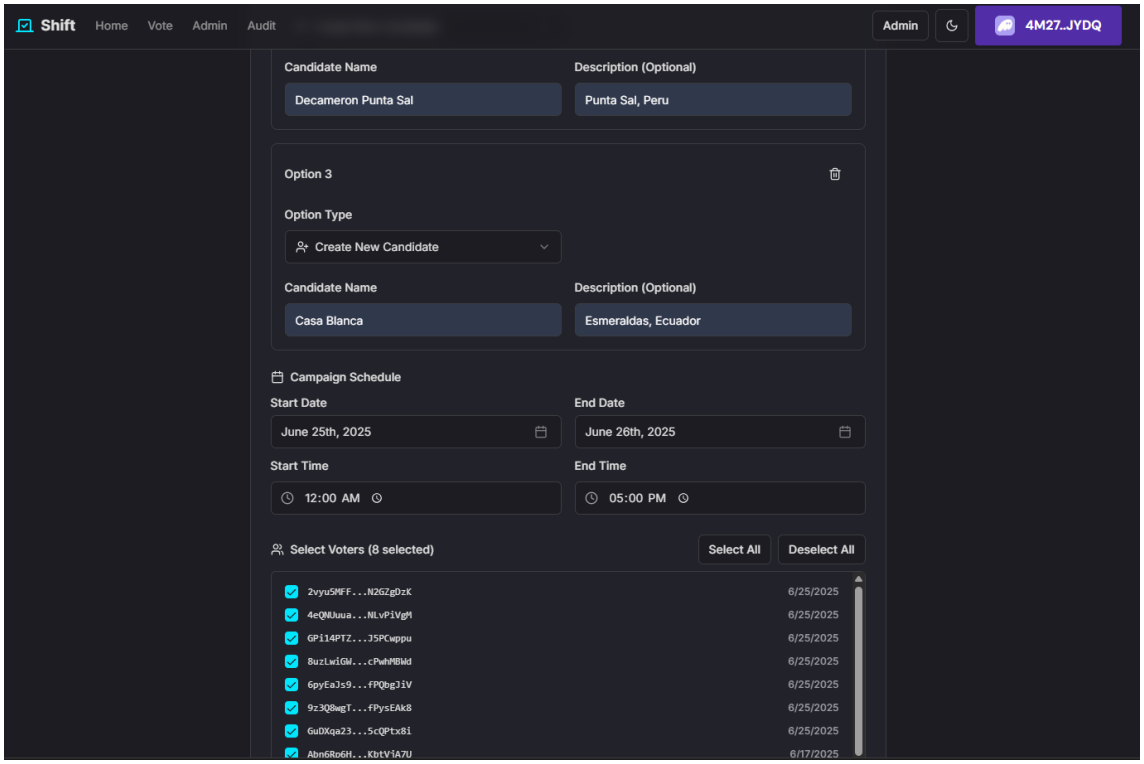
ANEXO 3. Resultados de pruebas en Smart Contract

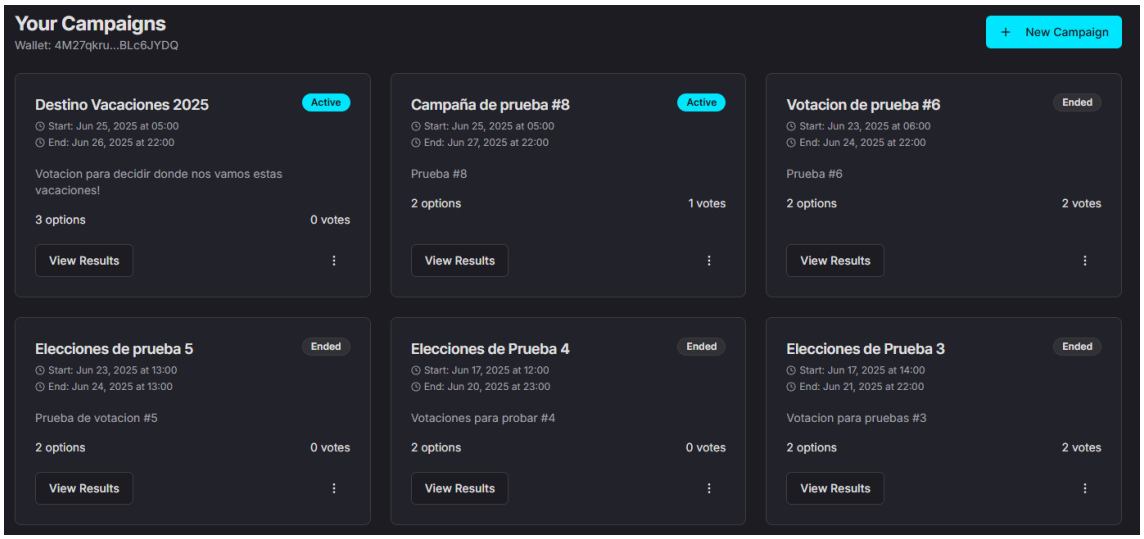


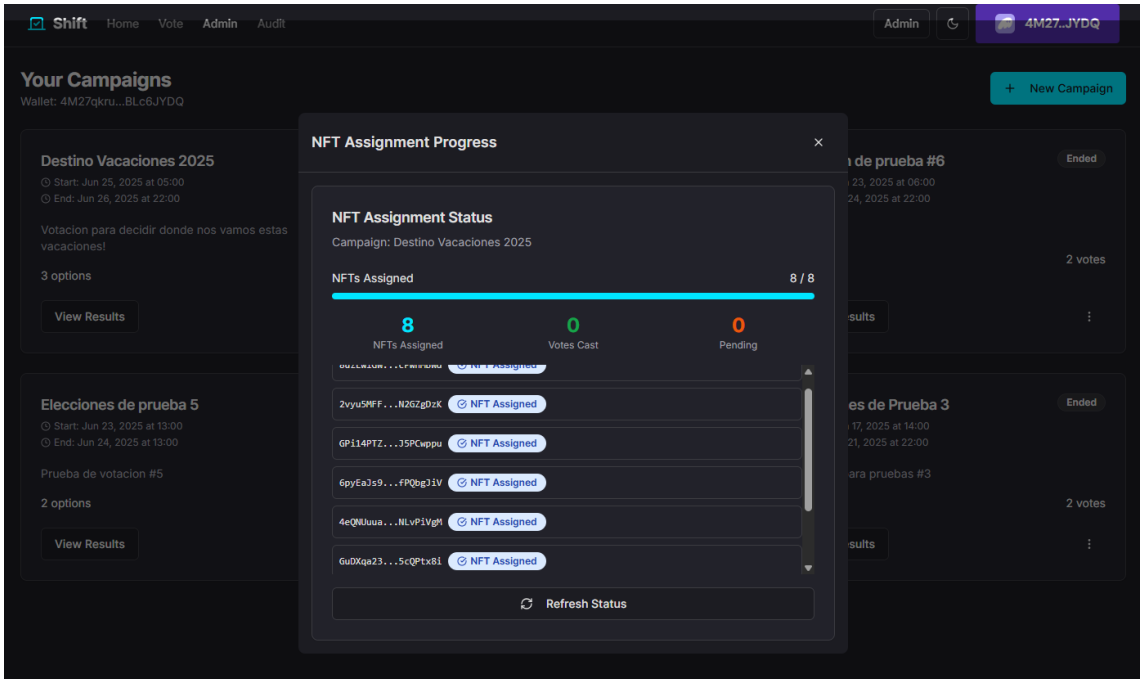
ANEXO 4. Simulación de campaña en Devnet

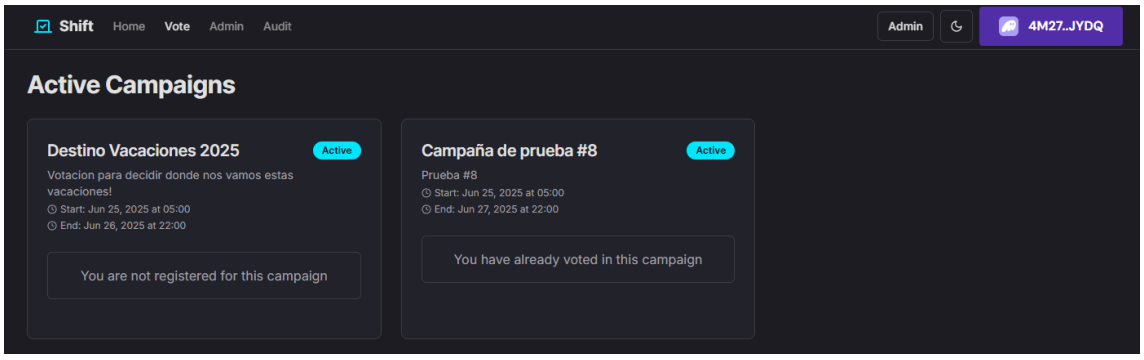


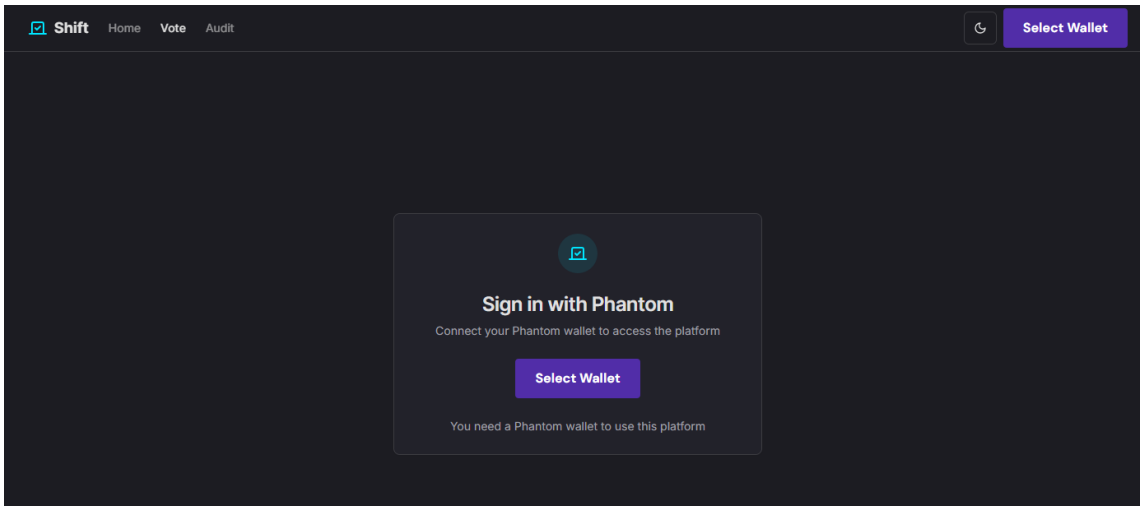

Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Create New Campaign
Create New Campaign
Set up a new voting campaign with custom options and selected voters
Campaign Title
Destino Vacaciones 2025
Description (Optional)
Votacion para decidir donde nos vamos estas vacaciones!
Voting Options
Add Option
Option 1
Option Type
Create New Candidate
Candidate Name
Decameron Mompiche
Description (Optional)
Mompiche, Ecuador
Option 2
Option Type
Create New Candidate

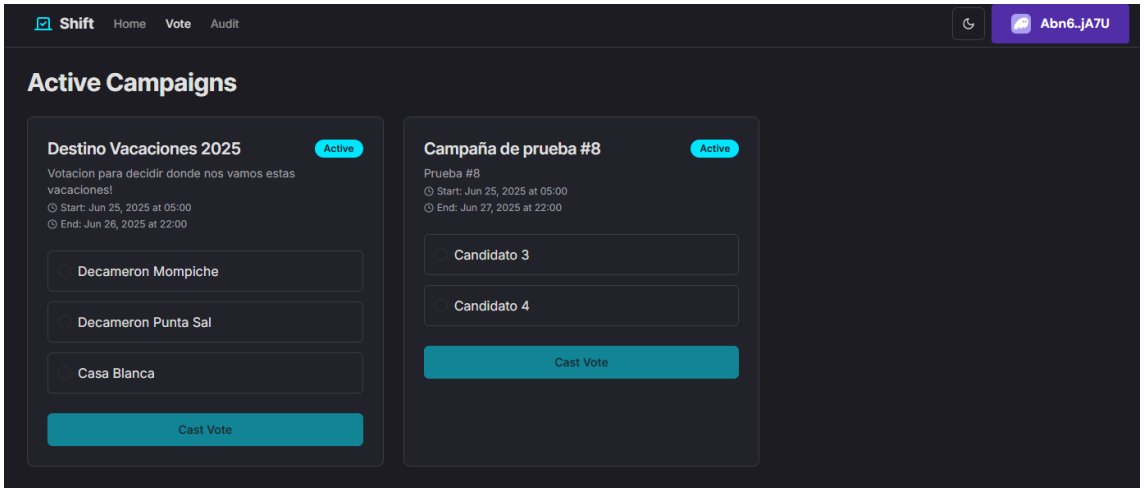

Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Candidate Name
Decameron Punta Sal
Description (Optional)
Punta Sal, Peru
Option 3
Option Type
Create New Candidate
Candidate Name
Casa Blanca
Description (Optional)
Esmeraldas, Ecuador
Campaign Schedule
Start Date
June 25th, 2025
End Date
June 26th, 2025
Start Time
12:00 AM
End Time
05:00 PM
Select Voters (8 selected)
Select All
Deselect All
2vyu5MFF...N2GZgDzK 6/25/2025
4eQNUuua...NLvPiVgM 6/25/2025
GPi14PTZ...J5PCwppu 6/25/2025
8uzLwiGW...cPwhMBWd 6/25/2025
6pyEaJs9...fPQbgJiV 6/25/2025
9z3Q8wgT...fPysEAk8 6/25/2025
6uDXqa23...5cQPtx8i 6/25/2025
Abn6Ro6H...KbtViA7U 6/17/2025

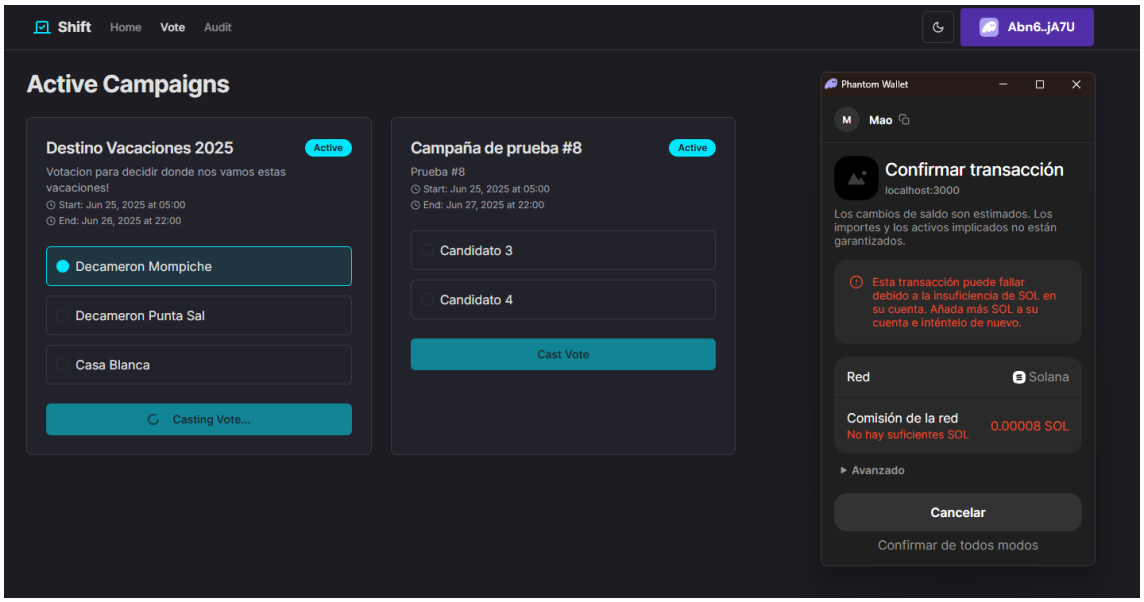

Your Campaigns
Wallet: 4M27qkru...BLc6JYDQ
New Campaign
Destino Vacaciones 2025
Active
Start: Jun 25, 2025 at 05:00
End: Jun 26, 2025 at 22:00
Votacion para decidir donde nos vamos estas vacaciones!
3 options
0 votes
View Results
Campaña de prueba #8
Active
Start: Jun 25, 2025 at 05:00
End: Jun 27, 2025 at 22:00
Prueba #8
2 options
1 votes
View Results
Votacion de prueba #6
Ended
Start: Jun 23, 2025 at 06:00
End: Jun 24, 2025 at 22:00
Prueba #6
2 options
2 votes
View Results
Elecciones de prueba 5
Ended
Start: Jun 23, 2025 at 13:00
End: Jun 24, 2025 at 13:00
Prueba de votacion #5
2 options
0 votes
View Results
Elecciones de Prueba 4
Ended
Start: Jun 17, 2025 at 12:00
End: Jun 20, 2025 at 23:00
Votaciones para probar #4
2 options
0 votes
View Results
Elecciones de Prueba 3
Ended
Start: Jun 17, 2025 at 14:00
End: Jun 21, 2025 at 22:00
Votacion para pruebas #3
2 options
2 votes
View Results

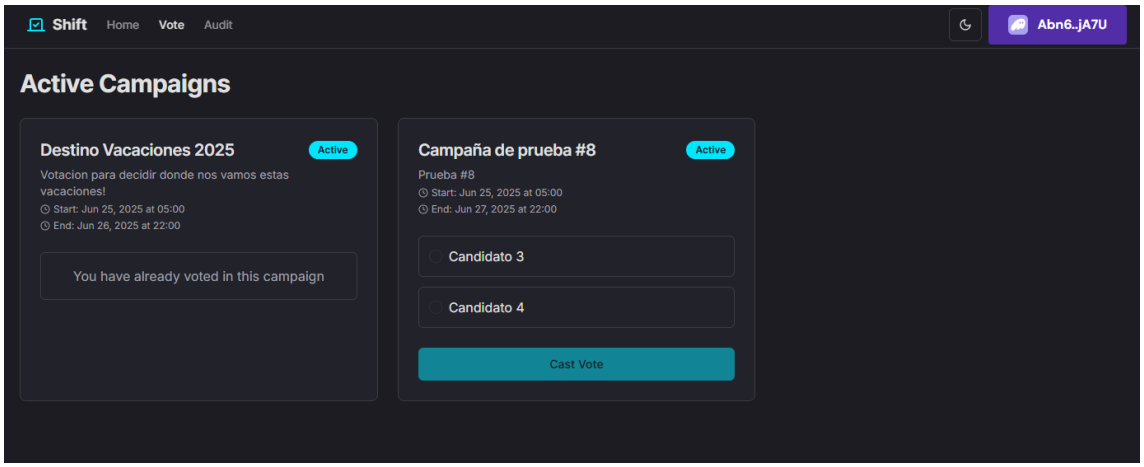

Shift
Home
Vote
Admin
Audit
Admin
4M27...JYDQ
Your Campaigns
Wallet: 4M27qkru...BLc6JYDQ
New Campaign
NFT Assignment Progress
NFT Assignment Status
Campaign: Destino Vacaciones 2025
NFTs Assigned
8 / 8
8
NFTs Assigned
0
Votes Cast
0
Pending
2vyu5MFF...N2GZgDzK
NFT Assigned
GPi14PTZ...J5PCwppu
NFT Assigned
6pyEaJs9...fPQbgJiV
NFT Assigned
4eQNUuua...NLvPiVgM
NFT Assigned
GuDXqa23...5cQPtx8i
NFT Assigned
Refresh Status
Destino Vacaciones 2025
Elecciones de prueba 5
Elecciones de Prueba 3

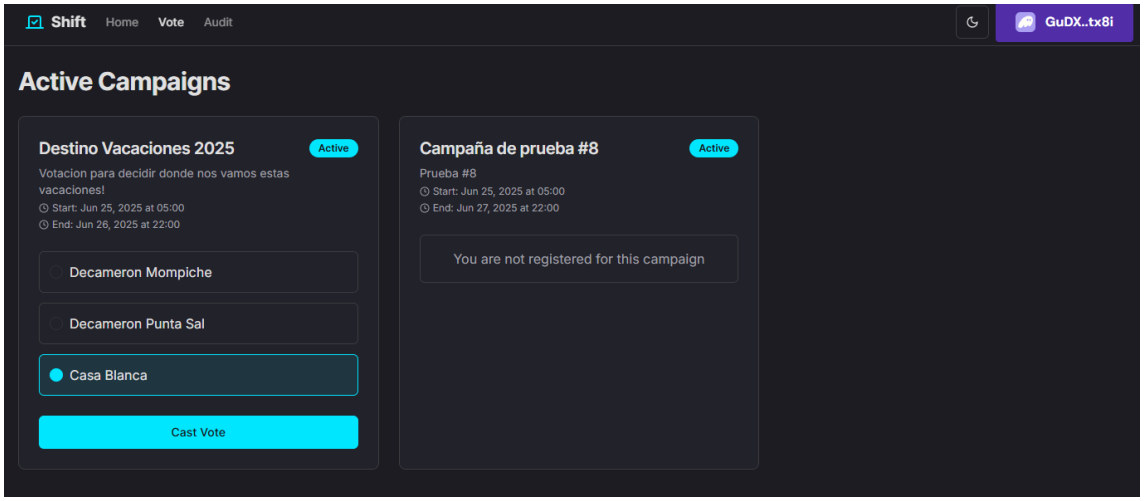

Shift
Home
Vote
Admin
Audit
Admin
4M27...JYDQ
Active Campaigns
Destino Vacaciones 2025
Active
Votacion para decidir donde nos vamos estas vacaciones!
Start: Jun 25, 2025 at 05:00
End: Jun 26, 2025 at 22:00
You are not registered for this campaign
Campaña de prueba #8
Active
Prueba #8
Start: Jun 25, 2025 at 05:00
End: Jun 27, 2025 at 22:00
You have already voted in this campaign

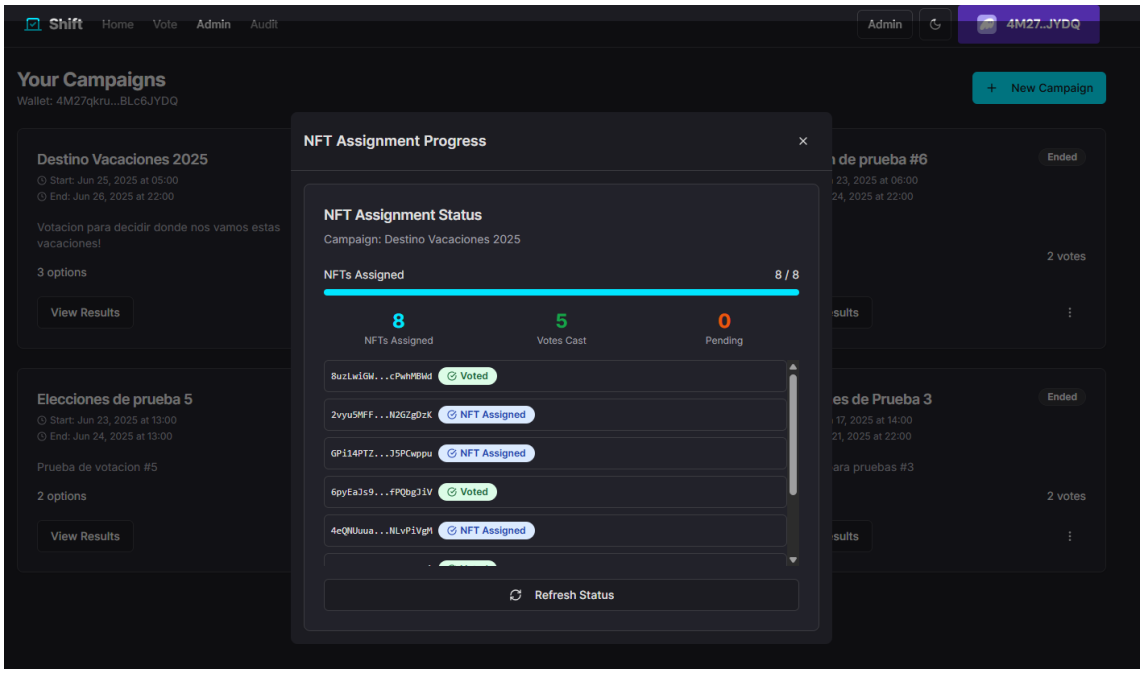

Shift
Home
Vote
Audit
Select Wallet
Sign in with Phantom
Connect your Phantom wallet to access the platform
Select Wallet
You need a Phantom wallet to use this platform

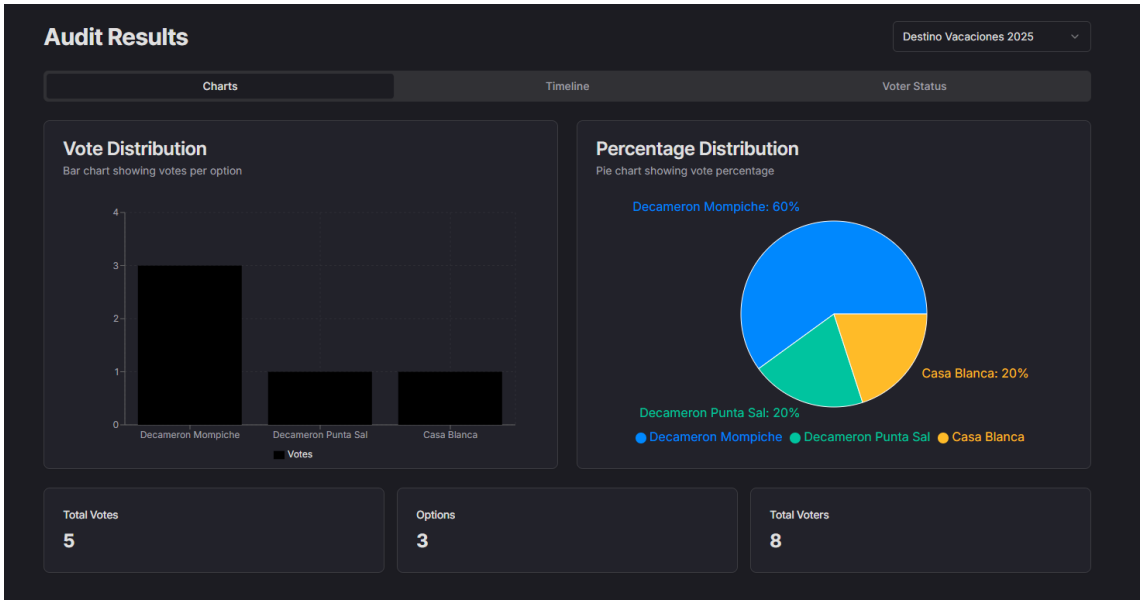

Shift
Home
Vote
Audit
Abn6..jA7U
Active Campaigns
Destino Vacaciones 2025
Active
Votacion para decidir donde nos vamos estas vacaciones!
Start: Jun 25, 2025 at 05:00
End: Jun 26, 2025 at 22:00
Decameron Mompiche
Decameron Punta Sal
Casa Blanca
Cast Vote
Campaña de prueba #8
Active
Prueba #8
Start: Jun 25, 2025 at 05:00
End: Jun 27, 2025 at 22:00
Candidato 3
Candidato 4
Cast Vote


Shift
Home
Vote
Audit
Abn6..jA7U
Active Campaigns
Destino Vacaciones 2025
Active
Votacion para decidir donde nos vamos estas vacaciones!
Start: Jun 25, 2025 at 05:00
End: Jun 26, 2025 at 22:00
Decameron Mompiche
Decameron Punta Sal
Casa Blanca
Casting Vote...
Campaña de prueba #8
Active
Prueba #8
Start: Jun 25, 2025 at 05:00
End: Jun 27, 2025 at 22:00
Candidato 3
Candidato 4
Cast Vote
Phantom Wallet
Mao
Confirmar transacción
localhost:3000
Los cambios de saldo son estimados. Los importes y los activos implicados no están garantizados.
Esta transacción puede fallar debido a la insuficiencia de SOL en su cuenta. Añada más SOL a su cuenta e inténtelo de nuevo.
Red
Solana
Comisión de la red
No hay suficientes SOL
0.00008 SOL
Avanzado
Cancelar
Confirmar de todos modos

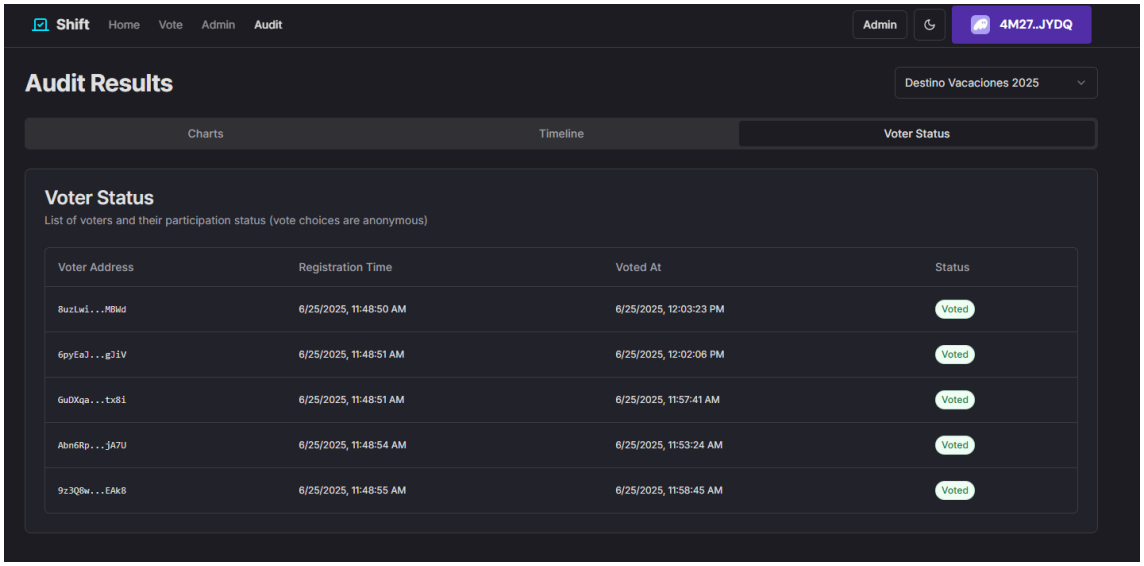

Shift
Home
Vote
Audit
Abn6..jA7U
Active Campaigns
Destino Vacaciones 2025
Active
Votacion para decidir donde nos vamos estas vacaciones!
Start: Jun 25, 2025 at 05:00
End: Jun 26, 2025 at 22:00
You have already voted in this campaign
Campaña de prueba #8
Active
Prueba #8
Start: Jun 25, 2025 at 05:00
End: Jun 27, 2025 at 22:00
Candidato 3
Candidato 4
Cast Vote


Shift
Home
Vote
Audit
GuDX..tx8i
Active Campaigns
Destino Vacaciones 2025
Active
Votacion para decidir donde nos vamos estas vacaciones!
Start: Jun 25, 2025 at 05:00
End: Jun 26, 2025 at 22:00
Decameron Mompiche
Decameron Punta Sal
Casa Blanca
Cast Vote
Campaña de prueba #8
Active
Prueba #8
Start: Jun 25, 2025 at 05:00
End: Jun 27, 2025 at 22:00
You are not registered for this campaign


Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Your Campaigns
Wallet: 4M27qkru...BLc6JYDQ
New Campaign
Destino Vacaciones 2025
Start: Jun 25, 2025 at 05:00
End: Jun 26, 2025 at 22:00
Votacion para decidir donde nos vamos estas vacaciones!
3 options
View Results
NFT Assignment Progress
NFT Assignment Status
Campaign: Destino Vacaciones 2025
NFTs Assigned
8 / 8
8
NFTs Assigned
5
Votes Cast
0
Pending
8uzLwiGW...cPwhMBWd
Voted
2vyu5MFF...N2GZgDzK
NFT Assigned
GPi14PTZ...J5PCwppu
NFT Assigned
6pyEaJs9...fPQbgJiV
Voted
4eQNUuua...NLvPiVgH
NFT Assigned
Refresh Status
de prueba #6
Ended
2 votes
Elecciones de prueba 5
Start: Jun 23, 2025 at 13:00
End: Jun 24, 2025 at 13:00
Prueba de votacion #5
2 options
View Results
es de Prueba 3
Ended
2 votes


Audit Results
Destino Vacaciones 2025
Charts
Timeline
Voter Status
Vote Distribution
Bar chart showing votes per option
4
3
2
1
0
Decameron Mompiche
Decameron Punta Sal
Casa Blanca
Votes
Percentage Distribution
Pie chart showing vote percentage
Decameron Mompiche: 60%
Casa Blanca: 20%
Decameron Punta Sal: 20%
Decameron Mompiche
Decameron Punta Sal
Casa Blanca
Total Votes
5
Options
3
Total Voters
8


Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Voting Timeline
Vote progression over time for each candidate
By Minute
4
3
2
1
0
Jun 25, 04:49 PM
Jun 25, 04:50 PM
Jun 25, 04:51 PM
Jun 25, 04:52 PM
Jun 25, 04:53 PM
Jun 25, 04:54 PM
Jun 25, 04:55 PM
Jun 25, 04:56 PM
Jun 25, 04:57 PM
Jun 25, 04:58 PM
Jun 25, 04:59 PM
Jun 25, 05:00 PM
Jun 25, 05:01 PM
Jun 25, 05:02 PM
Jun 25, 05:03 PM
Jun 25, 05:04 PM
Jun 25, 05:05 PM
Jun 25, 05:06 PM
Decameron Mompiche
Decameron Punta Sal
Casa Blanca


Shift
Home
Vote
Admin
Audit
Admin
4M27..JYDQ
Audit Results
Destino Vacaciones 2025
Charts
Timeline
Voter Status
Voter Status
List of voters and their participation status (vote choices are anonymous)
Voter Address
Registration Time
Voted At
Status
8uzLwi...MBWd
6/25/2025, 11:48:50 AM
6/25/2025, 12:03:23 PM
Voted
6pyEaJ...gJiV
6/25/2025, 11:48:51 AM
6/25/2025, 12:02:06 PM
Voted
GuDXqa...tx8i
6/25/2025, 11:48:51 AM
6/25/2025, 11:57:41 AM
Voted
Abn6Rp...jA7U
6/25/2025, 11:48:54 AM
6/25/2025, 11:53:24 AM
Voted
9z3Q8w...EAk8
6/25/2025, 11:48:55 AM
6/25/2025, 11:58:45 AM
Voted