"La Técnica al Servicio de la Patria"

Diseño de un sistema de votación digital basado en blockchain

Presenta:
Emmanuel Campos Genaro

Asesores:
Yolanda Victoria Hernandez
Luis Antonio Garcia Espinosa

Instituto Politécnico Nacional
Escuela Superior de Ingeniería Mecánica y Eléctrica
Especialidad en Computación

Mexico, CDMX
2024

"Blockchain es la herramienta tecnológica que puede devolver la confianza en las instituciones, al hacer transparentes los procesos y asegurar que cada acción sea verificable."

- Don Tapscott

Agradecimientos

Dedicar años de esfuerzo y estudio para alcanzar la meta de convertirme en Ingeniero no hubiera sido posible sin el apoyo incondicional de muchas personas que estuvieron a mi lado en este viaje. Por ello, deseo expresar mi más profundo agradecimiento a todos aquellos que contribuyeron a hacer realidad este sueño.

En primer lugar, mi gratitud eterna a mi familia, cuyo amor, paciencia y confianza en mí nunca flaquearon. Desde mi nacimiento hasta hoy, han creído en mis sueños, objetivos y metas, apoyándome en cada paso del camino. A mis padres, por sus sacrificios y por creer en mí incluso cuando los desafíos parecían insuperables. A mi hermano menor David, quien no solo ha sido mi apoyo constante sino también mi mentor y compañero en varios emprendimientos.

Un agradecimiento especial a mis profesores y mentores del Instituto, cuya sabiduría y dedicación no solo me formaron como profesional, sino que también me inspiraron a ser mejor persona. Gracias por desafiar mis límites, alimentar mi curiosidad y guiarme con paciencia a través del complejo mundo de la ingeniería.

A mis amigos y compañeros de estudio, gracias por todas las jornadas de trabajo en equipo, por compartir conocimientos, risas y cafés, que hicieron más llevaderos los momentos de estrés y cansancio. Su amistad y apoyo han sido pilares fundamentales en este camino.

Finalmente, agradezco a la vida misma por darme la oportunidad de cumplir este objetivo y por todos los aprendizajes adquiridos en el camino. Este logro no solo simboliza el cierre de un capítulo importante en mi vida, sino también el inicio de una nueva etapa llena de retos y oportunidades.

Con el corazón lleno de gratitud, me comprometo a ejercer mi profesión con integridad, buscando siempre contribuir al desarrollo de mi comunidad y el bienestar de la sociedad.

Índice general

Resumen

Este proyecto se centra en el diseño y desarrollo de un sistema de votación electrónica avanzado y seguro, implementando la tecnología blockchain para garantizar la integridad, transparencia y seguridad de los procesos electorales. Utilizando la plataforma Ethereum, el sistema emplea contratos inteligentes para gestionar las votaciones y asegurar la inmutabilidad de los resultados electorales.

La metodología de Design Thinking se aplica a lo largo del proyecto para garantizar que el diseño sea humanocéntrico y resuelva efectivamente las necesidades reales de los usuarios. Este enfoque facilita una iteración rápida y una adaptación continua del diseño basada en la retroalimentación, esencial para el desarrollo de soluciones tecnológicas en entornos electorales complejos.

Como parte de la metodología, se desarrollará un Proof-of-Concept para demostrar la viabilidad técnica y la eficacia del sistema de votación en un entorno real. Este prototipo inicial se implementará como una herramienta para instrumentos democráticos dentro del Instituto Politécnico Nacional, específicamente en la ESIME Zacatenco. Esta fase inicial permitirá evaluar el funcionamiento del sistema en un contexto controlado y académico antes de considerar su expansión a niveles más amplios de gobernanza electoral.

La revisión teórica del proyecto profundiza en la evolución de los sistemas de votación electrónica, destacando cómo los avances tecnológicos han permitido superar desafíos históricos como el fraude y la falta de confianza en los resultados. Se examina en detalle la estructura y los principios de la blockchain, explicando cómo la descentralización contribuye a la seguridad y transparencia electoral. Adicionalmente, se examina el impacto transformador del white paper de Satoshi Nakamoto en el ámbito de las criptomonedas y se reconoce la influencia decisiva de los Cypherpunks en la promoción de la privacidad digital y la seguridad a través de la criptografía avanzada.

Desde una perspectiva metodológica, el proyecto adopta el enfoque del Desarrollo Rápido de Aplicaciones (RAD), complementado con metodologías ágiles como la Programación Extrema (XP) y Kanban. Este enfoque integrado permite una iteración rápida y una adaptación continua del sistema basada en retroalimentación constante, lo cual es crucial para el desarrollo de soluciones tecnológicas en entornos electorales dinámicos.

En términos de desarrollo práctico, se describe la implementación técnica del sistema, que incluye desde la integración de hardware específico para la autenticación segura de votantes, hasta el desarrollo de interfaces de usuario amigables y accesibles. Se enfatiza el uso de Web3.js para la interacción eficiente y segura con la blockchain de Ethereum. Además, se detallan los procedimientos de pruebas exhaustivas diseñadas para validar la seguridad, la funcionalidad y la usabilidad del sistema.

El objetivo principal del proyecto es ofrecer un sistema de votación electrónica que no solo cumpla con los más altos estándares de seguridad y eficiencia, sino que también se distinga de los sistemas existentes en términos de facilidad de uso y confiabilidad. A través del análisis comparativo, se evalúan las ventajas competitivas y las limitaciones del sistema propuesto. El proyecto concluye proponiendo futuras líneas de investigación y mejoras del sistema, basadas en los resultados obtenidos y las tendencias emergentes en la tecnología electoral.

Este enfoque integral no solo subraya la importancia técnica de implementar soluciones basadas en blockchain, sino que también enfatiza la relevancia social y política de avanzar hacia sistemas electorales más robustos en tiempos de cambios significativos y desafíos democráticos en México. La convergencia de estos factores en las elecciones de 2024 y la implementación inicial en un contexto educativo como la ESIME Zacatenco ofrece un contexto único para evaluar y potencialmente transformar el panorama electoral mediante la adopción de tecnología avanzada, estableciendo un precedente para futuras iniciativas de modernización electoral tanto en México como en otros contextos internacionales.

Abstract

This thesis project focuses on the design and development of an advanced and secure electronic voting system, implementing blockchain technology to ensure the integrity, transparency, and security of electoral processes. Using the Ethereum platform, the system employs smart contracts to manage voting and ensure the immutability of electoral results.

The Design Thinking methodology is applied throughout the project to ensure that the design is human-centric and effectively addresses the real needs of users. This approach facilitates rapid iteration and continuous design adaptation based on feedback, which is essential for developing technological solutions in complex electoral environments.

As part of the methodology, a Proof-of-Concept will be developed to demonstrate the technical viability and effectiveness of the voting system in a real environment. This initial prototype will be implemented as a tool for democratic instruments within the National Polytechnic Institute, specifically at ESIME Zacatenco. This initial phase will allow the system's functionality to be evaluated in a controlled and academic context before considering its expansion to broader levels of electoral governance.

The theoretical review of the project delves into the evolution of electronic voting systems, highlighting how technological advances have overcome historical challenges such as fraud and lack of trust in the results. The structure and principles of the blockchain are examined in detail, explaining how decentralization contributes to electoral security and transparency. Additionally, the transformative impact of Satoshi Nakamoto's white paper in the field of cryptocurrencies is examined, and the decisive influence of the Cypherpunks in promoting digital privacy and security through advanced cryptography is acknowledged.

From a methodological perspective, the project adopts a Rapid Application Development (RAD) approach, complemented by agile methodologies such as Extreme Programming (XP) and Kanban. This integrated approach allows for rapid iteration and continuous system adaptation based on constant feedback, which is crucial for developing technological solutions in dynamic electoral environments.

In terms of practical development, the technical implementation of the system is described, including everything from the integration of specific hardware for secure voter authentication to the development of user-friendly and accessible interfaces. The use of Web3.js is emphasized for efficient and secure interaction with the Ethereum blockchain. Additionally, procedures for exhaustive testing designed to validate the system's security, functionality, and usability are detailed.

The main objective of the project is to provide an electronic voting system that not only meets the highest standards of security and efficiency but also stands out from existing systems in terms of ease of use and reliability. Through comparative analysis, the competitive advantages and limitations of the proposed system are evaluated. The project concludes by proposing future lines of research and system improvements, based on the results obtained and emerging trends in electoral technology.

This comprehensive approach not only underscores the technical importance of implementing blockchain-based solutions but also emphasizes the social and political relevance of advancing towards more robust electoral systems in times of significant changes and democratic challenges in Mexico. The convergence of these factors in the 2024 elections and the initial implementation in an educational context such as ESIME Zacatenco offers a unique setting to evaluate and potentially transform the electoral landscape through the adoption of advanced technology, setting a precedent for future electoral modernization initiatives both in Mexico and in other international contexts.

Lista de tablas

Lista de figuras

Lista de Códigos de Ejemplos

Lista de abreviaturas o símbolos

Capítulo 1

Introducción

Este primer capítulo establece el contexto, justifica la necesidad y describe los objetivos de la investigación centrada en el desarrollo de un sistema de votación electrónica innovador que utiliza la tecnología blockchain. Este sistema no solo busca revolucionar los métodos tradicionales de votación mejorando la seguridad, la transparencia y la eficiencia del proceso electoral, sino que también responde a un momento crucial en la historia política y social de México, en especial ante las próximas elecciones de 2024. Además, en una primera etapa de despliegue, el proyecto será implementado como una herramienta para instrumentos democráticos dentro del Instituto Politécnico Nacional, específicamente en la ESIME Zacatenco. Esto permitirá evaluar su funcionamiento en un entorno controlado y académico antes de considerar su expansión a niveles más amplios de gobernanza electoral.

El capítulo se organiza en torno a varias secciones clave: primero, se contextualiza el proyecto dentro del panorama actual de los sistemas de votación y las tecnologías emergentes; segundo, se justifica la relevancia del estudio en el marco de los desafíos contemporáneos que enfrenta México, especialmente la necesidad de procesos electorales más transparentes y seguros; tercero, se detallan los objetivos específicos que guiarán la investigación y el desarrollo del sistema propuesto; cuarto, se define el alcance del estudio, delimitando las expectativas y las limitaciones del proyecto, incluyendo su implementación inicial en la ESIME Zacatenco; y finalmente, se describe la estructura del documento, proporcionando un mapa para navegar los capítulos subsiguientes que desarrollarán cada aspecto de esta investigación.

Este enfoque integral no solo subraya la importancia técnica de implementar soluciones basadas en blockchain, sino que también enfatiza la relevancia social y política de avanzar hacia sistemas electorales más robustos en tiempos de cambios significativos y desafíos democráticos en México. La convergencia de estos factores en las elecciones de 2024 y la implementación inicial en un contexto educativo como la ESIME Zacatenco ofrece un contexto único para evaluar y potencialmente transformar el panorama electoral mediante la adopción de tecnología avanzada, estableciendo un precedente para futuras iniciativas de modernización electoral tanto en México como en otros contextos internacionales.

1.1. Contexto y Justificación

La confianza pública en los procesos electorales es un pilar fundamental de cualquier democracia. Sin embargo, esta confianza se ha visto erosionada no solo por los desafíos intrínsecos de los sistemas tradicionales de votación, como el fraude electoral y los errores de conteo, sino también por una creciente preocupación global respecto a la manipulación electoral y la interferencia extranjera. En México, a medida que nos acercamos a las elecciones de 2024, estas preocupaciones son especialmente pertinentes. La nación se encuentra en una encrucijada crucial, buscando fortalecer su democracia mientras se enfrenta a desafíos significativos en términos de integridad electoral y transparencia gubernamental.

En este contexto, la tecnología blockchain se destaca como una solución potencialmente transformadora. Su aplicación en el sistema de votación promete abordar varios de los problemas más persistentes y perniciosos de los métodos de votación convencionales, incluyendo la seguridad de los datos, la verificación de la identidad del votante y la transparencia del proceso de conteo de votos. La inmutabilidad y la descentralización son características de la blockchain que pueden servir para restaurar la fe en los sistemas electorales, asegurando que cada voto sea contado correctamente y sea verificable de manera independiente sin riesgo de alteración o fraude.

El desarrollo de un sistema de votación electrónica basado en blockchain no solo es técnica y socialmente relevante; también es oportuno. Las elecciones de 2024 representan una oportunidad para

implementar nuevas tecnologías que pueden mejorar significativamente la administración de los procesos electorales en México. Este proyecto, al ser pilotado inicialmente en un entorno escolar, ofrece una plataforma para probar y refinar la tecnología en un entorno controlado, educativo y significativamente menos complejo que el ámbito nacional, pero con el potencial de escalar y adaptarse a mayores desafíos electorales.

Además, este enfoque proactivo hacia la innovación electoral puede servir como un modelo para otras naciones que buscan mejorar la seguridad y la integridad de sus propios procesos electorales, estableciendo a México como un líder en la adopción de tecnologías avanzadas en gobernanza democrática.

En resumen, la justificación de este proyecto radica en su capacidad para enfrentar desafíos técnicos y éticos cruciales mediante la integración de tecnologías avanzadas, al tiempo que se alinea con un momento histórico de renovación política y social en México. La implementación de tales sistemas no solo es una respuesta a los desafíos actuales sino también una inversión en la resiliencia y evolución futura de las prácticas democráticas, especialmente en la víspera de una elección tan significativa como la de 2024.

1.2. Objetivos

1.2.1. Objetivo General

En una fase inicial, se diseñará y desarrollará un sistema de votación electrónica avanzado utilizando la tecnología blockchain y la plataforma Ethereum, específicamente adaptado para su implementación en un entorno escolar. Este sistema buscará mejorar de manera significativa la seguridad, la transparencia y la privacidad de los procesos electorales estudiantiles, estableciendo un modelo de votación digital que pueda ser validado y replicado en contextos más amplios. Centrándose en principios de descentralización y auditoría pública, el proyecto implementará contratos inteligentes para asegurar la inmutabilidad y la verificación independiente de los registros de votación, sin comprometer la privacidad de los votantes. A través del desarrollo de interfaces de usuario intuitivas y accesibles, este sistema pretende facilitar y maximizar la participación electoral de los estudiantes, mejorando su experiencia y educación cívica. Se realizarán pruebas exhaustivas dentro del entorno escolar para evaluar la funcionalidad, seguridad y escalabilidad del sistema. Adicionalmente, se comparará este sistema con métodos tradicionales de votación estudiantil para demostrar sus ventajas en seguridad, eficiencia y transparencia. Este objetivo inicial también incluirá la elaboración de directrices para la implementación y operación del sistema de votación electrónica en la escuela, proporcionando un marco que pueda ser adaptado y extendido a otros contextos electorales en el futuro.

1.2.2. Objetivos Específicos

1. Diseñar la arquitectura del sistema de votación para su uso en el entorno escolar, utilizando Ethereum y contratos inteligentes. Esta arquitectura debe asegurar la inmutabilidad y verificación pública de los votos, facilitando la integridad electoral y permitiendo auditorías fáciles y transparentes por parte de la comunidad educativa sin comprometer la privacidad de los estudiantes. 2. Desarrollar una interfaz de usuario amigable y educativa que no solo sea intuitiva y accesible para los estudiantes de todas las edades, sino que también les enseñe sobre el proceso de votación y los principios detrás de la blockchain. Esta interfaz deberá fomentar una mayor participación electoral y facilitar una mejor comprensión de la importancia de la seguridad y la transparencia en las elecciones. 3. Implementar medidas de seguridad robustas que estén adaptadas al contexto escolar, protegiendo el sistema contra fraudes y ataques cibernéticos. Estas medidas incluirán técnicas avanzadas de criptografía y autenticación que sean adecuadas para asegurar la confidencialidad y la integridad de los datos de votación, al tiempo que sean comprensibles y enseñables dentro del currículo escolar. 4. Realizar pruebas exhaustivas del sistema en un entorno controlado para evaluar su funcionalidad, seguridad y escalabilidad. Estas pruebas incluirán pruebas de carga y pruebas de aceptación de usuario realizadas por estudiantes y personal educativo, asegurando que el sistema cumple con los requisitos prácticos y educativos del entorno escolar. 5. Comparar el sistema desarrollado con los métodos de votación tradicionales usados en la escuela para demostrar las mejoras en términos de seguridad, eficiencia y transparencia. Este análisis ayudará a identificar las ventajas competitivas del sistema basado en blockchain y fomentará su aceptación entre los estudiantes y el personal educativo. 6. Elaborar directrices para la implementación y operación del sistema de votación electrónica en el entorno escolar, proporcionando un marco detallado que pueda ser utilizado para futuras implementaciones o adaptaciones en otros contextos educativos o electorales más

amplios. Este marco deberá incluir recomendaciones sobre aspectos técnicos, pedagógicos y regulatorios para facilitar una transición efectiva hacia sistemas de votación más modernos y seguros.

1.3. Alcances

- Desarrollo del Sistema: Diseño y creación de un sistema de votación electrónica que utilice la plataforma Ethereum y contratos inteligentes para gestionar y verificar los votos de manera segura y transparente.
- Entorno de Implementación: El sistema será implementado y probado inicialmente en un entorno escolar, con la participación de estudiantes y personal educativo en elecciones simuladas para validar su funcionalidad.
- Características del Sistema: Inclusión de una interfaz de usuario intuitiva y educativa que sea accesible para estudiantes de diversas edades. Implementación de medidas de seguridad robustas adaptadas a las necesidades y el contexto escolar.
- Pruebas de Funcionamiento: Realización de pruebas exhaustivas dentro de la escuela, incluyendo pruebas de carga, pruebas de aceptación de usuario, y pruebas de seguridad, para asegurar la funcionalidad y la fiabilidad del sistema.
- Análisis Comparativo: Comparación del sistema desarrollado con los sistemas de votación tradicionales utilizados en la escuela para evaluar las mejoras en seguridad, eficiencia y transparencia.
- Directrices de Implementación: Elaboración de un conjunto de directrices y recomendaciones para la implementación futura del sistema en otros contextos escolares o electorales.

1.4. Limitaciones

- Escala de Implementación: El proyecto se limitará inicialmente a un entorno escolar, lo que puede no representar completamente los desafíos encontrados en implementaciones a mayor escala en entornos más diversos.
- Recursos Tecnológicos: La disponibilidad de tecnología y la infraestructura de TI en la escuela pueden limitar la complejidad del sistema desarrollado o la amplitud de las pruebas realizables.
- Experiencia del Usuario: Las limitaciones en la experiencia previa de los usuarios (estudiantes y personal educativo) con tecnologías avanzadas como blockchain podrían afectar la adopción y la eficacia de la interfaz de usuario.
- Seguridad y Privacidad: Aunque se implementarán medidas de seguridad avanzadas, las limitaciones inherentes a cualquier sistema tecnológico, como posibles vulnerabilidades en software y hardware, podrían afectar la seguridad y privacidad de los datos.
- Aspectos Regulatorios y Legales: La implementación de un sistema de votación electrónica en un contexto real podría enfrentarse a desafíos legales y regulatorios que no serán completamente abordados en esta fase inicial.
- Dependencia de Terceros: El desarrollo del sistema depende de tecnologías y plataformas gestionadas por terceros (como Ethereum), lo que podría implicar restricciones relacionadas con cambios en sus protocolos o políticas.

1.5. Estructura del Documento

- Introducción
  - Contexto: Descripción del entorno actual de votación y sus desafíos.
  - Justificación: Por qué es importante y relevante desarrollar un sistema de votación basado en blockchain.
  - Objetivos del Proyecto: Tanto el objetivo general como los objetivos específicos.

- Alcance y Limitaciones: Detalles del alcance del proyecto y sus limitaciones.

- Marco Teórico
  - Historia de la Votación Electrónica: Evolución y desafíos anteriores.
  - Blockchain y Ethereum: Fundamentos, cómo funcionan, y su aplicación en sistemas de votación.
  - Seguridad en Sistemas de Votación: Importancia de la seguridad, métodos actuales, y cómo blockchain mejora esta área.
  - Aspectos Legales y Éticos: Consideraciones legales y éticas en la implementación de sistemas de votación electrónica.

- Metodología
  - Diseño del Sistema: Arquitectura general del sistema de votación utilizando blockchain.
  - Desarrollo del Software: Herramientas y tecnologías usadas; detalles del frontend y backend.
  - Desarrollo de la Interfaz de Usuario: Cómo se diseñará para ser intuitiva y accesible.
  - Implementación de Seguridad: Estrategias y tecnologías para asegurar la votación.
  - Planificación de Pruebas: Tipos de pruebas a realizar para validar la funcionalidad y seguridad.

- Desarrollo
  - Configuración de la Infraestructura: Preparación de los entornos de desarrollo y prueba.
  - Implementación de Contratos Inteligentes: Desarrollo y despliegue en la red Ethereum.
  - Desarrollo de la Interfaz: Creación de la interfaz de usuario conforme a las especificaciones de diseño.
  - Integración de Sistemas: Cómo se integrarán todos los componentes del sistema (frontend, backend, blockchain).

- Pruebas y Evaluación
  - Pruebas de Funcionamiento: Pruebas de seguridad, usabilidad y carga.
  - Evaluación de la Interfaz de Usuario: Recopilación de feedback de estudiantes y personal.
  - Análisis de Resultados: Evaluación de la efectividad, seguridad y aceptación del sistema.

- Comparación y Análisis
  - Comparación con Sistemas Tradicionales: Ventajas y desventajas respecto a métodos existentes.
  - Análisis de Mejoras Potenciales: Cómo se podría mejorar el sistema en futuras iteraciones.

- Conclusiones y Recomendaciones
  - Resumen de Hallazgos: Principales descubrimientos y logros del proyecto.
  - Recomendaciones para Implementaciones Futuras: Orientación basada en la experiencia adquirida.
  - Propuestas de Investigación Futura: Áreas para futuros estudios y desarrollo.

- Apéndices
  - Documentación Técnica: Detalles técnicos del sistema.
  - Códigos Fuente: Ejemplos de códigos desarrollados.
  - Materiales Educativos: Recursos utilizados para enseñar a los usuarios sobre el sistema.