UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Ingeniería en Sistemas Computacionales

IMPLEMENTACIÓN DE UN SISTEMA DE VOTACIÓN ELECTRÓNICA PARA FORTALECER EL PROCESO DE ESCRUTINIO UTILIZANDO BLOCKCHAIN.

Trabajo de grado previo a la obtención del título de Ingeniero en Sistemas Computacionales

Autor:

Alex Efraín Ipiales Chasiguano

Director:

PhD. Irving Marlon Reascos Paredes

Ibarra - Ecuador

2022

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100454236-9		
APELLIDOS Y NOMBRES:	Ipiales Chasiguano Alex Efraín		
DIRECCIÓN:	San Cristóbal Alto – Caranqui		
EMAIL:	aeipialesc@utn.edu.ec		
TELÉFONO FIJO:	-	**TELÉFONO MÓVIL:**	0986429157

DATOS DE LA OBRA	
TÍTULO:	IMPLEMENTACIÓN DE UN SISTEMA DE VOTACIÓN ELECTRÓNICA PARA FORTALECER EL PROCESO DE ESCRUTINIO UTILIZANDO BLOCKCHAIN
AUTOR (ES):	Ipiales Chasiguano Alex Efraín
FECHA: DD/MM/AAAA	06/05/2022
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniero en Sistemas Computacionales
ASESOR /DIRECTOR:	PhD. Irving Reascos

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 6 días del mes de mayo de 2022

EL AUTOR:

.....
Alex Efraín Ipiales Chasiguano
CI: 100454236-9

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN DEL DIRECTOR

Por medio de la presente yo PhD. Irving Reascos, certifico que el Sr. Alex Efraín Ipiales Chasiguano, portador de la cédula de identidad Nro.100454236-9, ha trabajado en el desarrollo del proyecto de tesis "**IMPLEMENTACIÓN DE UN SISTEMA DE VOTACIÓN ELECTRÓNICA PARA FORTALECER EL PROCESO DE ESCRUTINIO UTILIZANDO BLOCKCHAIN**", previo a la obtención del título de Ingeniería en Sistemas Computacionales, lo cual ha realizado en su totalidad con responsabilidad.

Es todo cuanto puedo certificar en honor de la verdad.

Atentamente:

1001501400
IRVING MARLON
REASCOS
PAREDES

Fecha:
2022.05.06
12:02:32
-05'00'

PhD. Irving Reascos

DIRECTOR DE TESIS

DEDICATORIA

El presente trabajo está dedicado especialmente a mis padres, quienes fueron los pilares principales de mi motivación y esfuerzo, además de su confianza, paciencia y su incondicional apoyo durante todo el transcurso de mi carrera universitaria.

A todos mis amigos y demás familiares quienes compartieron sus fuerzas, ánimos y esperanza, además de ser un incentivo para seguir mejorando y cumplir una meta más en mi vida.

Alex Ipiales

AGRADECIMIENTO

Agradezco profundamente a mis padres, quienes son mi fuente de inspiración para seguir adelante y quienes me enseñaron el valor de la perseverancia, a mis compañeros de la universidad con quienes me apoyaron en momentos difíciles y con los cuales compartí muchos momentos alegres.

De igual forma, agradezco a mi tutor PhD. Irving Reascos, que gracias a sus consejos y correcciones hoy puedo culminar este trabajo. A todos los docentes que, con su sabiduría, conocimiento y apoyo, motivaron a desarrollarme como persona y profesional en la Universidad Técnica del Norte.

TABLA DE CONTENIDO

DEDICATORIA ii
AGRADECIMIENTO v
TABLA DE CONTENIDO vi
ÍNDICE DE FIGURAS viii
ÍNDICE DE TABLAS x
RESUMEN xi
ABSTRACT xii
INTRODUCCIÓN 1
Antecedentes 1
Situación Actual 1
Prospectiva 1
Planteamiento del Problema 2
Objetivos 3
Objetivo General 3
Objetivos Específicos 3
Alcance 3
Justificación 4
Contexto 5
CAPÍTULO 1 8
Revisión de Literatura 8
1.1 Proceso de revisión de la literatura 8
1.1.1 Unidad de análisis y preguntas de investigación 8
1.1.2 Búsqueda de documentos 9
1.1.3 Selección de Artículos 9
1.1.4 Extracción de los datos relevantes 11
1.2 Resultados de la revisión de Literatura 13
1.2.1 Voto electrónico 13
1.2.2 Blockchain 16
1.2.3 Voto electrónico con blockchain 20
1.2.4 Beneficios de blockchain en el voto electrónico 21
1.2.5 Algoritmos de consenso 23
1.2.6 Contratos inteligentes 24
1.2.7 Desafíos de la tecnología blockchain 25
1.2.8 Plataformas blockchain que permiten contratos inteligentes 27
1.2.9 Productos blockchain en el mercado 30

CAPÍTULO 2 32
Desarrollo 32
2.1 Fase de Inicio Scrum 32
2.1.1 Definición de Roles 32
2.1.2 Definición del Product Backlog 32
2.2 Fase de planificación y estimación 34
2.2.1 Definición de historias de usuario 34
2.2.2 Planificación del proyecto 38
2.3 Desarrollo del proyecto 38
2.3.1 Tecnologías de desarrollo 38
2.3.2 Esquema de la aplicación 41
2.3.3 Planificación del sprint 1 42
2.3.4 Ejecución del sprint 1 43
2.3.5 Planificación del sprint 2 44
2.3.6 Ejecución del sprint 2 46
2.3.7 Planificación del sprint 3 50
2.3.8 Ejecución del sprint 3 51
2.3.9 Planificación del sprint 4 56
2.3.10 Ejecución del sprint 4 57
2.3.11 Planificación del sprint 5 61
2.3.12 Ejecución del sprint 5 62
CAPÍTULO 3 64
Resultados 64
3.1 Diseño del instrumento de medición 65
3.1.1 Planificación 65
3.1.2 Recolección de datos 66
3.1.3 Análisis de datos 67
3.2 Presentación de resultados 69
3.2.1 Análisis del perfil de los encuestados 69
3.2.2 Variables del modelo de DeLone y McLean (cuestionario para electores) 70
3.2.3 Análisis de favorabilidad y desfavorabilidad 76
3.2.4 Variables del modelo de DeLone y McLean (Administradores) 77
CONCLUSIONES 84
RECOMENDACIONES 86
LIMITACIONES Y TRABAJOS FUTUROS 87
REFERENCIAS 88
ANEXOS 91

ÍNDICE DE FIGURAS

Figura 1. Diagrama de planteamiento de problemas 2
Figura 1.1. Alcance del trabajo de titulación 4
Figura 1.2. Proceso de revisión de literatura 8
Figura 1.3. Modalidad de votación electrónica 13
Figura 1.4. Capas de blockchain 17
Figura 1.5. Estructura de un bloque 18
Figura 1.6. Proceso de una transacción en la blockchain 19
Figura 1.7. Proceso de votación con blockchain 21
Figura 1.8. Resumen de la red Ethereum 28
Figura 1.9. Resumen de la red BSC 29
Figura 1.10. Resumen de la red Polygon 30
Figura 2.1. Tecnologías utilizadas en el sistema 40
Figura 2.2. Diagrama de la aplicación 41
Figura 2.3. Caso de uso general del sistema 43
Figura 2.4. Colección de usuarios 43
Figura 2.5. Vista del login 44
Figura 2.6. Validación de los datos en el login 44
Figura 2.7. Caso de uso Gestión de elecciones 46
Figura 2.8. Caso de uso Gestión de listas 46
Figura 2.9. Colección de elecciones 47
Figura 2.10. Colección de listas de candidatos 47
Figura 2.11. Vista de elecciones 48
Figura 2.12. Advertencias al eliminar una elección 48
Figura 2.13. Formulario para ingresar o editar elecciones 48
Figura 2.14. Vista listas 49
Figura 2.15. Agregar listas desde un archivo Excel 49
Figura 2.16. Formulario para agregar listas 50
Figura 2.17. Advertencias al eliminar una lista 50
Figura 2.18. Caso de uso Gestión de candidatos 52
Figura 2.19. Caso de uso Gestión de usuarios 52
Figura 2.20. Colección de candidatos 53
Figura 2.21. Colección de cargos 53
Figura 2.22. Vista de candidatos 54
Figura 2.23. Creación de cargos para candidatos 54
Figura 2.24. Advertencias al eliminar y agregar candidato 55

Figura 2.25. Vista usuarios 55
Figura 2.26. Validaciones de cédula y correo 55
Figura 2.27. Caso de uso Efectuar voto 57
Figura 2.28. Habilitar voto nulo y blanco 58
Figura 2.29. Agregar listas a blockchain con Metamask 58
Figura 2.30. Verificación de elección activa 59
Figura 2.31. Vista para el sufragio 59
Figura 2.32. Enviar voto a la blockchain 60
Figura 2.33. Verificación del voto 60
Figura 2.34. Voto en la blockchain 61
Figura 2.35. Consultar resultados de la elección 62
Figura 2.36. Verificación de elección finalizada 62
Figura 2.37. Vista de resultados 63
Figura 3.1. Modelo de éxito de DeLone and McLean 64
Figura 3.2. Género de los encuestados 70
Figura 3.3. Edad de los encuestados 70
Figura 3.4. Calidad del sistema - Elector 71
Figura 3.5. Calidad de la información - Elector 72
Figura 3.6. Calidad del servicio - Elector 73
Figura 3.7. Intensión de uso - Elector 74
Figura 3.8. Satisfacción del usuario - Elector 75
Figura 3.9. Beneficios obtenidos - Elector 76
Figura 3.10. Calidad del sistema - Administrador 78
Figura 3.11. Calidad de la información - Administrador 79
Figura 3.12 Calidad del servicio - Administrador 80
Figura 3.13 Intensión de uso - Administrador 81
Figura 3.14. Satisfacción del usuario – Administrador 82
Figura 3.15. Beneficios obtenidos - Administrador 83
Figura 4.1. Variables declaradas en el contrato inteligente Vote 91
Figura 4.2. Contrato inteligente, función addLists 92
Figura 4.3. Contrato inteligente, función vote 92
Figura 4.4. Contrato inteligente, función winningList 92
Figura 4.5. Contrato inteligente, función winnerName 93
Figura 4.6. Descarga de Metamask 94
Figura 4.7. Creación de una cuenta en Metamask 94
Figura 4.8. Agregar nueva red en Metamask 95

ÍNDICE DE TABLAS

Tabla 1: Contextualización de trabajos de investigación 5
Tabla 1.1: Preguntas de Investigación planteadas 9
Tabla 1.2: Selección de artículos para la SLR 10
Tabla 1.3: Artículos seleccionados para la SLR 10
Tabla 1.4: Matriz de conceptos 12
Tabla 2.1: Asignación de roles Scrum 32
Tabla 2.2: Técnica T-Shirt Size 33
Tabla 2.3: Definición del Product Backlog 33
Tabla 2.4: Historia de Usuario 1 - Login Administrador 34
Tabla 2.5: Historia de Usuario 2 - Login Elector 34
Tabla 2.6: Historia de Usuario 3 - Gestión de Elecciones 35
Tabla 2.7: Historia de Usuario 4 - Gestión de listas 35
Tabla 2.8: Historia de Usuario 5 - Gestión de candidatos 35
Tabla 2.9: Historia de Usuario 6 - Gestión de usuarios 36
Tabla 2.10: Historia de Usuario 7 - Agregar listas a blockchain 36
Tabla 2.11: Historia de Usuario 8 - Efectuar voto 37
Tabla 2.12: Historia de Usuario 9 - Mostrar Resultados 37
Tabla 2.13: Planificación del proyecto por Sprints 38
Tabla 2.14: Sprint 1 – Desarrollo del login del administrador/elector 42
Tabla 2.15: Sprint 2 - Gestión de elecciones y listas 45
Tabla 2.16: Sprint 3 - Gestión candidatos y votantes 50
Tabla 2.17: Sprint 4 - Efectuar voto 56
Tabla 2.18: Sprint 5 - Mostrar Resultados 61
Tabla 3.1: Definición de las preguntas del cuestionario por dimensión 65
Tabla 3.2: Interpretación del coeficiente alfa de Cronbach 67
Tabla 3.3: Matriz de datos - resultados del cuestionario 67
Tabla 3.4: Coeficiente total de fiabilidad 68
Tabla 3.5: Resultados del Alfa de Cronbach 68
Fuente: Obtenido de software IBM SPSS statistics 26 68
Tabla 3.6: Resultados de favorabilidad por dimensión 77

RESUMEN

Actualmente, existen diversos sistemas de voto electrónico que tienen beneficios como: ahorro ecológico, eficiencia en el proceso de escrutinio y accesibilidad para los electores extranjeros. Sin embargo, a causa de la inserción de la tecnología dentro de un proceso electoral, también han surgido vulnerabilidades y ataques a estos sistemas informáticos, lo cual disminuye la confianza y participación en estos sistemas. Para afrontar dichas deficiencias, se propone utilizar la tecnología blockchain juntamente con los contratos inteligentes, los cuales mediante su estructura descentralizada e inmutable nos proveen una solución.

El objetivo general del presente trabajo de titulación fue el desarrollo de un sistema web para el voto electrónico basado en blockchain que garantice la integridad de datos y confiabilidad en un proceso electoral, enfocado principalmente en el uso de contratos inteligentes para el proceso de sufragio, escrutinio y emisión de resultados.

En primer lugar, se realizó una revisión bibliográfica centrada en el voto electrónico y la tecnología blockchain con sus respectivas características, funcionamiento y beneficios, así como también los contratos inteligentes y algunas plataformas blockchain a utilizar para dar solución al problema.

Para el desarrollo del sistema se utilizó la metodología Scrum, la cual proporcionó una mejora continua del sistema a través de sus iteraciones. En este contexto, se inició con la definición de roles, las historias de usuario, y posteriormente se planificó los Sprints con sus respectivas tareas hasta finalizar con el desarrollo.

Para medir el éxito y eficacia del sistema desarrollado se realizó la validación mediante el modelo de éxito de DeLone y McLean, considerando las categorías de: calidad del sistema, calidad de la información, calidad del servicio, intensión de uso, satisfacción del usuario y sus impactos netos, obteniendo resultados mayormente positivos, es decir, un sistema exitoso.

Palabras clave: voto electrónico, blockchain, contratos inteligentes, plataformas blockchain, proceso electoral.

ABSTRACT

Currently, there are several electronic voting systems that have benefits such as: ecological savings, efficiency in the counting process and accessibility for foreign voters. However, due to the insertion of technology within an electoral process, vulnerabilities and attacks have also arisen to these computer systems, which decreases trust and participation in these systems. To address these shortcomings, it is proposed to use blockchain technology together with smart contracts, which through their decentralized and immutable structure provide us with a solution.

The general objective of this titling work was the development of a web system for electronic voting based on blockchain that guarantees data integrity and reliability in an electoral process, focused mainly on the use of smart contracts for the process of suffrage, counting and issuance of results.

First, a bibliographic review was carried out focused on electronic voting and blockchain technology with their respective characteristics, operation, and benefits, as well as smart contracts and some blockchain platforms to be used to solve the problem.

For the development of the system, the Scrum methodology was used, which provided a continuous improvement of the system through its iterations. In this context, it began with the definition of roles, user stories, and then the Sprints were planned with their respective tasks until the development was completed.

To measure the success and effectiveness of the system developed, validation was carried out using the success model of DeLone and McLean, considering the categories of quality of the system, quality of information, quality of service, intention of use, user satisfaction and its net impacts, obtaining mostly positive results, that is, a successful system.

Keywords: electronic voting, blockchain, smart contracts, blockchain platforms, electoral process.

INTRODUCCIÓN

Antecedentes

Durante muchos años el derecho al voto ha sido un pilar fundamental en nuestra sociedad, debido a que es el medio para elegir nuevos gobernantes tanto a nivel del país como también de instituciones o empresas que requieran un gobierno democrático. En las últimas elecciones presidenciales se ha evidenciado inconvenientes que reducen la transparencia y credibilidad de un proceso electoral debido a que se presentan actas con inconsistencia, esto generalmente ocurre cuando las actas están sin firma del presidente o secretario de la mesa de votación, fallas de escaneo, inconsistencias numéricas o tienen reclamos de organizaciones políticas. (Mella, 2021).

La persistencia de inconsistencias genera un reconteo como también una demora en los resultados finales. Sin embargo, también se presentan inconvenientes a nivel tecnológico, principalmente relacionados con la inaccesibilidad a la página de publicación de resultados a causa de la concurrencia de usuarios (Noboa, 2017a).

Situación Actual

En la actualidad los ciudadanos, empresas y estados están incursionando con una gama de tecnologías, sin embargo, las instituciones y empresas pequeñas no cuentan con un sistema que facilite el proceso de escrutinio para obtener resultados más rápidos debido a consideraciones que plantean, “como el costo alto de los equipos e infraestructura de operación, seguridad del sistema, intromisiones de personas no autorizadas y a lo que algunos llaman la “deshumanización” del acto de votación” (Places, 2017).

Además, se plantean más consideraciones relacionados con la conectividad y disponibilidad de energía eléctrica para no perder información o que el sistema se detenga por causas externas al software. A causa de que los procesos necesitan una infraestructura tecnológica grande, las instituciones y pequeñas empresas optan por el proceso tradicional o manual que requiere personal humano para el proceso 9 electoral.

Prospectiva

Para el presente proyecto de titulación se propone desarrollar un sistema de voto electrónico para pequeñas instituciones u organizaciones mediante tecnologías que permiten evitar la manipulación de datos que se han dado en elecciones populares pasadas, generando retrasos en los resultados. La propuesta tendrá como base la aplicación de la

tecnología blockchain para bajar el índice de inconsistencias en el proceso de escrutinio, garantizando la integridad de datos y seguridad del proceso, de la misma manera con los resultados que se obtengan al final de la jornada democrática.

Planteamiento del Problema

Las elecciones populares son consideradas un pilar fundamental para tener una sociedad democrática donde las personas tienen libre expresión de voluntad de los electores para designar un nuevo representante de una institución u organización. A pesar del avance tecnológico las instituciones y pequeñas organizaciones no han incorporado un sistema que permita agilitar el proceso electoral debido a que los costos son muy elevados y su implementación requiere de una infraestructura grande.

A consecuencia se sigue optando por el voto tradicional, obteniendo una extensa jornada electoral lo que ocasiona errores en el proceso de escrutinio que exige un extenso recuento de las papeletas, esta problemática retrasa la publicación de resultados generando desconfianza por parte de los candidatos y participantes que ha futuro pierden la credibilidad e importancia de la transparencia en las elecciones (Noboa, 2017b).

Figura 1. Diagrama de planteamiento de problemas

Objetivos

Objetivo General

Desarrollar un sistema web para el voto electrónico basado en blockchain que garantice la integridad de datos y confiabilidad en un proceso electoral.

Objetivos Específicos

1. Definir el estado del arte del uso de blockchain en el voto electrónico a través de una revisión de literatura.
2. Desarrollar el sistema de voto electrónico con la tecnología blockchain para generar un proceso confiable.
3. Validar el producto desarrollado usando el modelo de éxito de los sistemas de información de DeLone y McLean

Alcance

En el presente anteproyecto se propone analizar la tecnología blockchain y su incidencia en los sistemas de votación electrónica. Además, se desarrollará una prueba de concepto que genere agilidad en el proceso y se obtengan resultados de manera rápida y confiables.

Este sistema se pretende desarrollar en modalidad web y altamente parametrizable que tendrá dos tipos de usuarios: administrador y votante. El usuario administrador podrá realizar la gestión de elecciones, candidatos y votantes con las funciones de registrar, modificar, eliminar y consultar. El usuario votante podrá ingresar al sistema, elegir el candidato de su preferencia y enviar su voto. En este proceso se podrá monitorizar el avance de las elecciones hasta su culminación, obteniendo resultados rápidos y confiables.

Se utilizará Scrum al ser una metodología de desarrollo ágil que tiene como base la idea de creación de ciclos breves para el desarrollo, que comúnmente se llaman iteraciones y que en Scrum se llamaran “Sprints” (Jimenez, 2018). Para su validación, se realizará una prueba de concepto en alguna organización o institución pequeña que realice un proceso electoral para elegir un nuevo representante, delimitado especialmente para elección de candidatos y la aplicación de blockchain para la inmutabilidad de votos.

Para la implementación de este sistema web se hará uso de las siguientes herramientas:

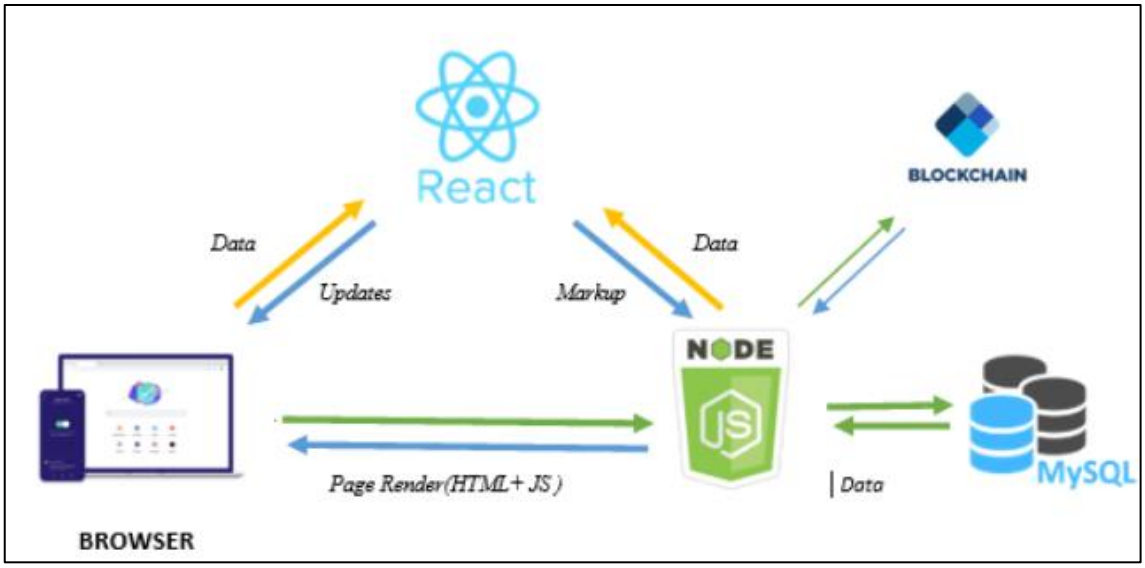


Figura 1.1. Alcance del trabajo de titulación

Justificación

La implementación de este trabajo de titulación a través del voto electrónico mediante la tecnología blockchain ayudará a la solución de uno de los objetivos de Desarrollo Sostenible, los objetivos ODS N°17 "Garantizar la adopción en todos los niveles de decisiones inclusivas, participativas y representativas que respondan a las necesidades" que tiene como una de sus metas "Garantizar la adopción en todos los niveles de decisiones inclusivas, participativas y representativas que respondan a las necesidades" (CEPAL, 2018). Todo esto con el fin de fomentar la participación a todos los ciudadanos en la toma de decisiones.

Dentro del Plan Nacional Toda Una Vida, el presente proyecto va apalancado con el objetivo N°7: Incentivar una sociedad participativa, con un Estado cercano al servicio de la ciudadanía, con referencia a la democratización y libertad para elegir nuevos representantes en diferentes estancias. (CEPAL, 2018)

Justificación Tecnológica

El presente trabajo de titulación tiene como principal objetivo automatizar el proceso de votación manual mediante un sistema web que disminuirá los errores en el proceso de escrutinio, además de proveer los resultados de manera rápida, ahorrando tiempo y costos en personal humano. También se implementará la tecnología blockchain para mejorar la seguridad de los datos, respetando los principios de la votación en especial el de integridad.

La gran ventaja de Blockchain es que permite registrar una transacción, contrato o cualquier otro tipo de actuación en internet de manera verificable, infalsificable y transparente,

sin necesidad de que un tercero verifique su validez. Además, permite sumar a la cadena con la misma fiabilidad el historial de evolución que pueda tener ese acuerdo (España, 2018).

Justificación Ambiental

El proyecto ayudará a disminuir la desforestación causada por el uso del papel lo que también conlleva el cambio climático para las generaciones futuras, asegurando una mejor calidad de vida y ecosistema. de calidad de información, calidad de sistema y calidad de servicio (Vega, 2018).

Contexto

El presente tema de investigación pretende contextualizar los conocimientos previamente establecidos en los trabajos de investigación enmarcados en la Tabla 1.

Tabla 1: Contextualización de trabajos de investigación

INVESTIGACIÓN	ENLACE	APORTE
Sistema de voto electrónico con protocolos de curvas elípticas aplicado en elecciones populares	http://repositorio.utn.edu.ec/handle/123456789/7581	A diferencia del protocolo de curvas elípticas, la investigación propuesta implementará blockchain para asegurar la integridad de los datos.
Sistema de recolección de votos electrónicos a través de interfaz natural de usuario	http://repositorio.utn.edu.ec/handle/123456789/9547	En lugar de implementar una interfaz natural de usuario, la investigación propuesta se basa en la seguridad mediante una base de datos descentralizada.
Estudio de factibilidad para desarrollo e implementación del voto electrónico en la Universidad Católica de Santiago de Guayaquil.	http://repositorio.ucsg.edu.ec/handle/3317/1300?locale=fr	A diferencia del estudio de factibilidad nuestra propuesta se basa en la implementación y desarrollo de software.

Implementación del voto electrónico para la Asociación de Profesores Universidad Católica Santiago de Guayaquil (APUC-G)	http://repositorio.ucsg.edu.ec/handle/3317/3781?locale=fr	A diferencia del desarrollo de software de un sistema de voto electrónico, nuestra propuesta se basa en mejorar la confiablidad mediante la aplicación de las características de blockchain.
Propuesta tecnológica para la sistematización del proceso de voto electoral estudiantil dentro de la unidad educativa particular dante alighieri del distrito 3 de la ciudad de guayaquil.	http://repositorio.ug.edu.ec/handle/redug/19633	Básicamente se trata de una propuesta para el proceso electoral mientras que la investigación propuesta se basa en la implantación de una nueva tecnología en un sistema de voto electrónico.
El voto electrónico en el Ecuador, perspectivas desde crecientes avances tecnológicos	https://rus.ucf.edu.cu/index.php/rus/article/view/2129	Análisis de factibilidad de implementación del voto electrónico a diferencia del análisis, se propone estudiar los principios de voto electrónico y aplicarlos mediante blockchain.
Implementación de un prototipo de una red descentralizada blockchain para el voto electrónico en la universidad de guayaquil	http://repositorio.ug.edu.ec/handle/redug/33172	A diferencia de nuestro enfoque de inmutabilidad de datos, este prototipo no utiliza herramientas que generen una red descentralizada verificable.

Sistema de votación mediante blockchain	http://castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/316/TFG%20Marta%20Blanco%20Caama%C3%B1o.pdf?sequence=1&isAllowed=y	En lugar de realizar un prototipo con la única función del voto, nuestra propuesta implementará la gestión de candidatos, elecciones y usuarios, mediante la cual obtendremos un sistema altamente parametrizable.

CAPÍTULO 1

Revisión de Literatura

1.1 Proceso de revisión de la literatura

La revisión sistemática de literatura (RSL) es un método para identificar, analizar e interpretar investigación relevante en un campo determinado, el proceso de revisión utilizado fue propuesto por Jane & Richard (2002) en su artículo "Analyzing the past to prepare for the future: writing a literature review". El proceso consta de 4 pasos.

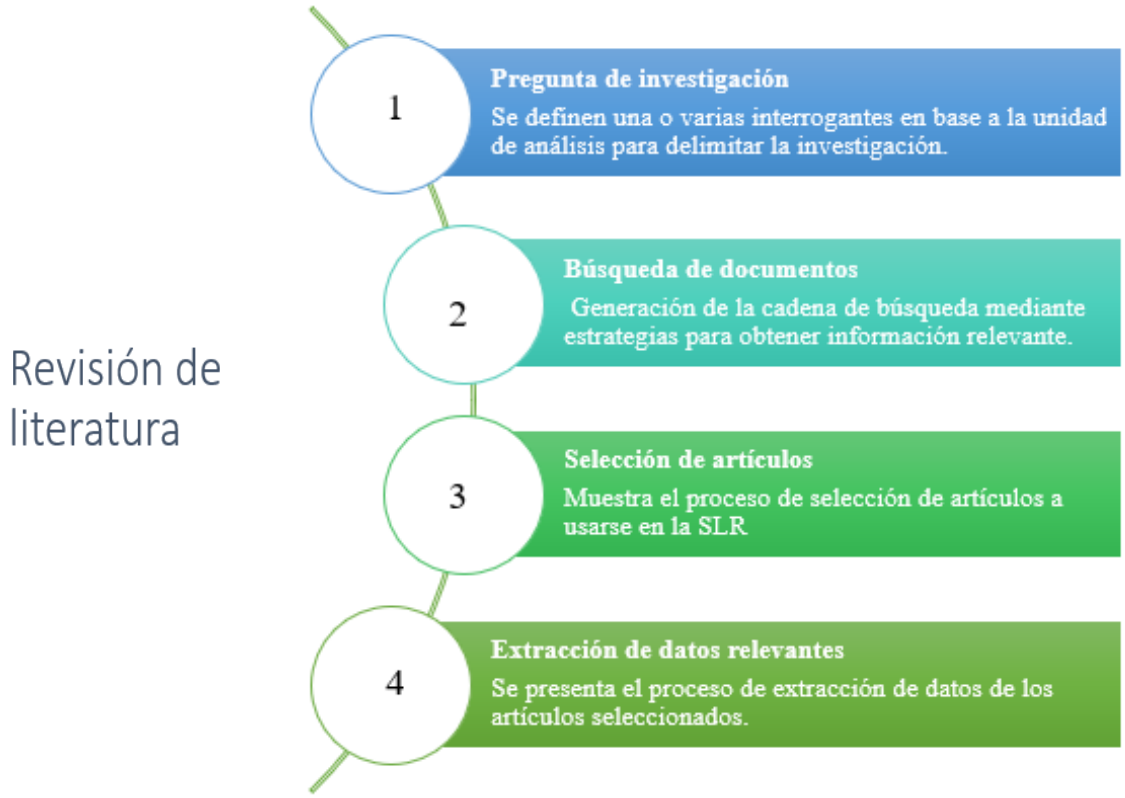


Figura 1.2. Proceso de revisión de literatura
Fuente (Jane & Richard, 2002)

A continuación, se expone el desarrollo de cada fase de la figura 1.2.

1.1.1 Unidad de análisis y preguntas de investigación

Unidad de análisis: Voto electrónico usando blockchain

Para el desarrollo de este proceso se estableció cuatro preguntas de investigación en referencia a la unidad de análisis, tabla 1.1, la mismas que servirán como pilares primordiales en el proceso de revisión de literatura. Además, se establecieron tres bases de datos bibliográficos a las cuales tiene acceso la Universidad Técnica del Norte, las cuales son: Scopus, IEEE, ScienceDirect.

Tabla 1.1: Preguntas de Investigación planteadas

Preguntas de Investigación	Motivación
¿Cuáles son las características que debe tener un sistema de voto electrónico?	La pregunta de investigación hace referencia a las características principales debe poseer un sistema de voto electrónico.
¿Qué beneficios atribuye la tecnología blockchain al voto electrónico?	La pregunta de investigación hace referencia al uso de blockchain como medio para fortalecer el proceso electoral aprovechando sus características.
¿Software existente para el voto electrónico usando blockchain?	La pregunta de investigación se centra en los sistemas de votación existentes y sus características con blockchain.
¿Cuáles son los desafíos que se presentan al usar la tecnología blockchain?	La pregunta de investigación se centra en los desafíos que se pueden presentar al usar blockchain en el voto electrónico.

1.1.2 Búsqueda de documentos

En la búsqueda de documentos se define la cadena de búsqueda en referencia a las preguntas de investigación previamente planteadas con la finalidad de encontrar información para responderlas. A continuación, se muestra la cadena de búsqueda usada en las bases de datos bibliográficas ya definidas anteriormente.

(“e-voting" OR "electronic vote" OR "electronic voting”) AND (“blockchain” OR “Smart contract” OR “Ethereum” OR “decentralized technology” OR “Web 3.0”) AND (“Software” OR “application” OR “features” OR “security” OR “advantage” OR “secure”)

1.1.3 Selección de Artículos

El proceso de selección de artículos tiene tres fases primordiales para obtener los artículos que tienen mayor aporte, en base a las preguntas de investigación. En la primera

fase se emplearon algunos criterios de inclusión y exclusión. Todos los artículos encontrados están relacionados con las siguientes disciplinas: Ciencias de la computación, ingeniería y tecnología, publicados con un máximo de 5 años de antigüedad (2017-2021) en preferencia del idioma inglés. En la segunda fase se excluyeron temas ajenos como: algoritmos de minería, criptografía y criptomonedas. Finalmente, en la tercera fase se realizó una revisión del resumen y el contenido del artículo para comprobar si responde a las preguntas de investigación previamente planteadas. Al finalizar el proceso de selección obtuvimos los siguientes resultados:

Tabla 1.2: Selección de artículos para la SLR

Base de datos	Fase 1	Fase 2	Fase 3
Scopus	23	9	6
IEEE	6	3	2
ScienceDirect	21	13	10
Total	**50**	**25**	**18**

En la siguiente tabla se enlistan los artículos seleccionados para realizar la revisión de literatura.

Tabla 1.3: Artículos seleccionados para la SLR

Código del Articulo	Titulo	Autor
A1	Architecture-Centric Evaluation of Blockchain-BasedSmart Contract E-Voting for National Elections	Olawande Daramola, Darren Thebus,
A2	Blockchain for Electronic Voting System—Review and Open Research Challenges	Uzma Jafar, Mohd, Juzaiddin & Zarina Shukur
A3	A Decentralized E-Voting System Based on Blockchain Network	Park, Hee-Dong
A4	A Secure Digital E-Voting Using Blockchain Technology	Geetha S, Sathya Sakthi Sree T
A5	Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharing	Yousif Abuidris, Rajesh Kumar, Ting Yang & Joseph Onginjo
A6	Highly Secured Blockchain Based Electronic Voting System Using SHA3 and Merkle Root	S Aruna, M Maheswari & A Saranya
A7	Go-Ethereum for electronic voting system using clique as proof-of-authority	Basilius Christyono, Moeljono Widjaja
A8	Trends in blockchain-based electronic voting systems	Pawlak & Michał Poniszewska

A9	Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities	Yang, Xuechao Yi, Andrei Han
A10	Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability	Zhang, Shufan Wang & Lili Xiong
A11	Investigating performance constraints for blockchain based secure e-voting system	Khan, Kashif Mehboob Arshad, Junaid Khan
A12	Trustworthy Electronic Voting Using Adjusted Blockchain Technology	Shahzad Basit, Crowcroft, Jon
A13	Survey on blockchain based smart contracts: Applications, opportunities, and challenges	Tharaka Hewa, Mika Ylianttilaa & Madhusanka Liyanage
A14	Blockchain 3.0 applications survey	DamianoDi Francesco Maesa
A15	SecureBallot: A secure open source e-Voting system	Agate, Vincenzo De Paola, Alessandra Ferraro
A16	Scalable blockchains — A systematic review	Nasir, Muhammad Hassan Arshad, Junaid Khan, Muhammad
A17	Blockchain as a sustainability-oriented innovation?: Opportunities for and resistance to Blockchain technology as a driver of sustainability in global food supply chains	Friedman, Nicola Ormiston, Jarrod
A18	Sidechain technologies in blockchain networks: An examination and state-of-the-art review	Singh, Amritraj Click, Kelly Parizi, Reza M.

1.1.4 Extracción de los datos relevantes

En el proceso de extracción de los datos relevantes se centra en los conceptos referente al voto electrónico con blockchain como unidad de análisis. En la tabla 1.4 se presentan los conceptos generales en relación con la tecnología blockchain para responder las preguntas de investigación planteadas.

Tabla 1.4: Matriz de conceptos

Código	Voto electrónico	Blockchain	Voto electrónico y blockchain	Beneficios de blockchain	Algoritmos de consenso	Contratos inteligentes	Desafíos de blockchain	Plataformas blockchain	Software existente
A1				X	X	X			
A2				X	X				
A3		X							X
A4					X			X	
A5							X	X	
A6				X					
A7			X					X	
A8						X	X		
A9	X		X			X			
A10						X	X		
A11			X	X					
A12					X				X
A13				X	X				X
A14							X		X
A15					X			X	
A16	X								
A17		X							
A18							X		

A continuación, se presentan los resultados con el objetivo de responder las preguntas de investigación propuestas, la información recaba está centrada en la unidad de análisis para considerar la implementación de la tecnología en el ámbito de la democracia.

1.2 Resultados de la revisión de Literatura

1.2.1 Voto electrónico

Generalmente, existen varias formas de conceptualizar el voto electrónico, pero todas coinciden en el uso de recursos informáticos. El voto electrónico a diferencia del tradicional utiliza medios electrónicos para automatizar las diferentes etapas del proceso electoral tales como: emisión, conteo y resultados. Además, es considerado como un medio de comunicación para la ciudadanía, por la presentación de resultados por medio de internet. El voto electrónico mediante una planificación adecuada puede mejorar ciertos aspectos del proceso electoral como: mayor eficacia, emisión de resultados, mayor comodidad al sufragar desde cualquier lugar mediante un dispositivo con conexión a internet y reducción de errores debido a menor interacción humana .

Modalidad de votación electrónica

El voto electrónico se divide en dos categorías, entornos controlados o presenciales, donde intervienen máquinas de votación y no controlados o remotos, los cuales no necesitan de máquinas de votación, ni un lugar específico para sufragar.

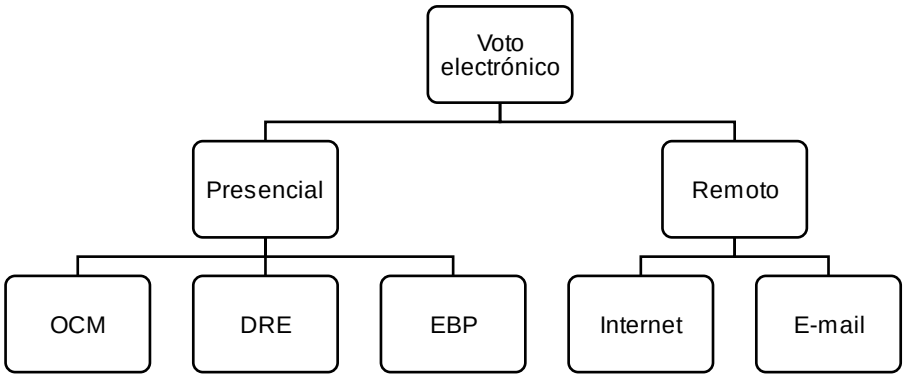


Figura 1.3. Modalidad de votación electrónica
Fuente (Elaboración propia)

Sistema de votación en entornos controlados (Presencial)

Se denominan entornos controlados debido a que los electores deben dirigirse a los recintos para sufragar, donde estarán supervisados por el organismo electoral, de esta manera se puede controlar en cierta forma las condiciones y procedimientos que debe cumplir un elector al sufragar, similar al voto tradicional con la diferencia del uso de máquinas de votación para la emisión del voto. Existen diferentes mecanismos de votación en un sistema presencial o controlado que son:

DRE (Registro electrónico de votos)

Son máquinas de votación donde el elector puede seleccionar el candidato de su preferencia mediante una pantalla táctil o en su defecto por medio de botones, donde su voto se registrará de manera electrónica similares a las urnas tradicionales.

ORM (Máquinas de lectura ópticas)

Estas máquinas son utilizadas para el proceso de conteo de votos, debido a que se encargan de escanear e identificar las papeletas marcadas por cada elector para posteriormente realizar la contabilización en un sistema que puede ser centralizado o descentralizado, en el primero, los datos se envían a una maquina central de manera directa y en el segundo, se recolectan los datos de cada recinto para finalmente ser enviados a un sistema central (Pawlak & Poniszewska-Marańda, 2021).

EBP (Impresoras de papeletas electrónicas)

Este tipo de sistema combina las dos anteriores, debido a que genera un comprobante electrónico con la opción elegida por el elector que posteriormente es introducido en un lector óptico para su respectivo conteo.

Sistema de votación en entornos no controlados (Remoto)

Básicamente denominados entornos no controlados o no supervisados debido a que la emisión del voto puede realizarse desde cualquier dispositivo con conexión a internet, si bien aumenta la comodidad del elector también tiene una gran cantidad de desafíos, como principal tenemos la incoercibilidad, donde al no tener supervisión, el voto puede verse afectado por personas externas que pueden interferir en la decisión del elector, cabe resaltar que no se puede realizar el reconteo debido a que el elector se queda con el comprobante de sufragio (Agate et al., 2021). Además, esta modalidad presenta varias controversias en cuanto a seguridad debido a la manipulación de información, reduciendo la confianza y por ende la transparencia del proceso electoral, de la misma manera no dispone de un recuento y no afianza el proceso de auditoría.

Ventajas

Los resultados de implementar un sistema de votación electrónico pueden influir de manera positiva en la sociedad como en la parte técnica, agilizando el proceso y consigo algunos aspectos de la votación tradicional como la participación y confianza en el sistema.

Ventajas sociales

Esta modalidad brinda varios beneficios, en especial a las personas con algún tipo de discapacidad o personas analfabetas, que pueden elegir al candidato de su preferencia a través de imágenes, asimismo, ayuda a personas con discapacidad visual mediante "audio-votos". Además, es un gran beneficio en cuanto a comodidad ya que pueden sufragar desde sus casas o en su defecto las personas que vivan en el extranjero. El tener una interfaz más intuitiva, puede disminuir el porcentaje de papeletas nulas, ya que el sistema brindas las instrucciones correspondientes para el correcto sufragio de su preferencia, mediante advertencias antes de enviar el voto (Agate et al., 2021).

Ventajas técnicas

Entre los beneficios más relevantes está, menor tiempo de escrutinio debido a que el recuento de los votos no se realiza de manera manual por lo cual se obtiene una mayor precisión en los resultados como también su presentación, de la misma manera reduce la participación de técnicos, supervisores y ciudadanos los cuales trabajan toda la jornada electoral hasta su culminación, haciendo todo este proceso de forma manual. Además, afecta positivamente al medio ambiente, al disminuir el uso de papel (Agate et al., 2021).

Mejoras en la participación y eficiencia del proceso electoral

El voto electrónico tiene como una de las promesas la ampliación de la participación a través de la reducción del abstencionismo electoral, con la accesibilidad que brinda la modalidad de votación remota desde cualquier dispositivo y lugar. Además, puede prevenir fraudes y realizar todo el proceso más rápido sin la intervención humana, evitando errores de tabulación de resultados.

Desventajas/Riesgos

A pesar de tener una mayor accesibilidad, presenta varias controversias en cuanto a la confiabilidad del proceso electoral y de la misma forma la seguridad del sistema (Pawlak & Poniszewska-Marańda, 2021).

- Poca transparencia
- Falta de comprensión en el uso del sistema para un público nuevo.
- Vulnerabilidad a ataques y manipulación de los votos por usuarios con privilegios al sistema.
- Menor control por parte del organismo electoral debido a la dependencia del proveedor del sistema o tecnología implementada.

- Mayores requerimientos tanto en infraestructura como en seguridad como en costos por el mantenimiento del sistema.

Requisitos

Los sistemas de voto electrónico presentan varios beneficios y también incertidumbre ante un público que desconoce el proceso de integridad de la información, en este caso se presentan características mínimas que deben ser aplicadas con el fin de obtener un efecto positivo en la aceptación de esta modalidad de sufragio (Olawande & Darren, 2020).

- El sistema de votación debe ofrecer la característica de integridad de información(votos).
- El sistema debe permitir el sufragio a personas que se encuentren registradas para el proceso de votación, excluyendo a personas externas para que registren su voto.
- El sistema debe cumplir con la característica de disponibilidad, haciendo posible que los electores puedan sufragar en todo momento y de manera simultánea durante el proceso de votación.
- El sistema debe ser justo en cuanto a la publicación de resultados, por lo tanto, no debe mostrar resultados parciales para no afectar la decisión de los votantes.
- El sistema debe garantizar el anonimato para obtener mayor seguridad en los votantes.
- El sistema debe garantizar la verificación del voto emitido, por tanto, cada elector puede conocer si su voto esta contabilizado en el proceso.
- El sistema debe garantizar transparencia para obtener un estado de aceptación por el público en general.

1.2.2 Blockchain

El concepto y tecnología de cadenas de bloques fue introducido por primera vez en 2009 por Satoshi Nakamoto, el creador de Bitcoin, considerada como la primera red blockchain con la finalidad de proveer un método de pago electrónico. Blockchain fue desarrollada para solventar el problema del doble gasto de las monedas digitales (Nasir et al., 2022). Esta tecnología está basada en el registro de información de manera distribuida en una red Peer-to-peer (P2P), donde todos los participantes de la red, denominados nodos, comparten su información y su confianza radica en los protocolos de consenso, quienes son los encargados de garantizar la seguridad y veracidad de la información en la red blockchain. Esta tecnología soluciona la dependencia de una entidad central para almacenar información o realizar transacciones de manera segura.

El termino blockchain, define la forma en que funciona esta tecnología, como una cadena, donde toda la información verificada mediante los nodos es almacenada en bloques, posteriormente estos bloques son agregados de forma ordenada a la cadena de bloques global, actualizando su estado (Friedman & Ormiston, 2022). Además, debido a su característica descentralizada, toda la información agregada es inmutable, haciendo imposible alterar la información. Finalmente, se puede destacar los atributos principales como: seguridad, transparencia, descentralización y eficacia, en base a la estructura, componentes y capas que maneja esta tecnología las cuales están expuestas en la figura 5.

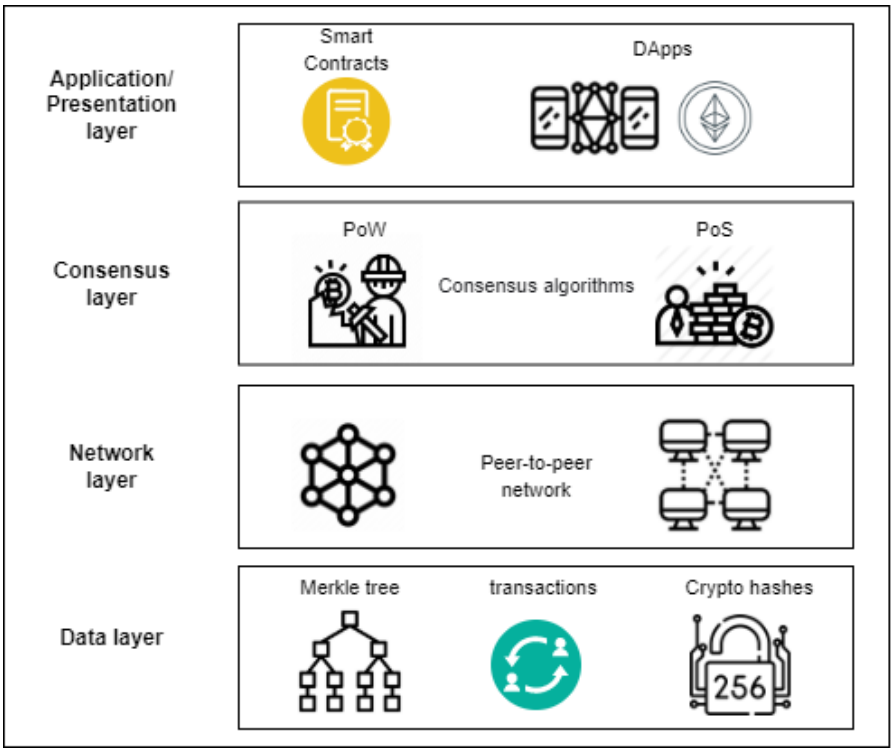


Figura 1.4. Capas de blockchain
Fuente (Elaboración propia)

Capa de datos

En esta capa se presenta la estructura de la cadena de bloques como se muestra en la figura 1.5, donde el primer bloque es llamado Genesis y a diferencia de los demás, no cuenta con el hash del bloque anterior. En este proceso las transacciones verificadas son almacenadas dentro de un bloque, estos bloques están vinculados mediante un hash del bloque anterior para garantizar la inmutabilidad de la información. Cada bloque se divide en dos partes, encabezado y cuerpo. El encabezado de un bloque contiene: el hash del bloque anterior, timestamp, nonce y el merkle root el cual es un hash que representa todas las transacciones dentro de un bloque mediante un algoritmo criptográfico denominado SHA-256, donde la generación del hash depende del contenido y un mínimo cambio, genera un hash

completamente diferente, haciendo énfasis en la integridad de la información. Mientras que el cuerpo del bloque contiene las transacciones (Nasir et al., 2022).

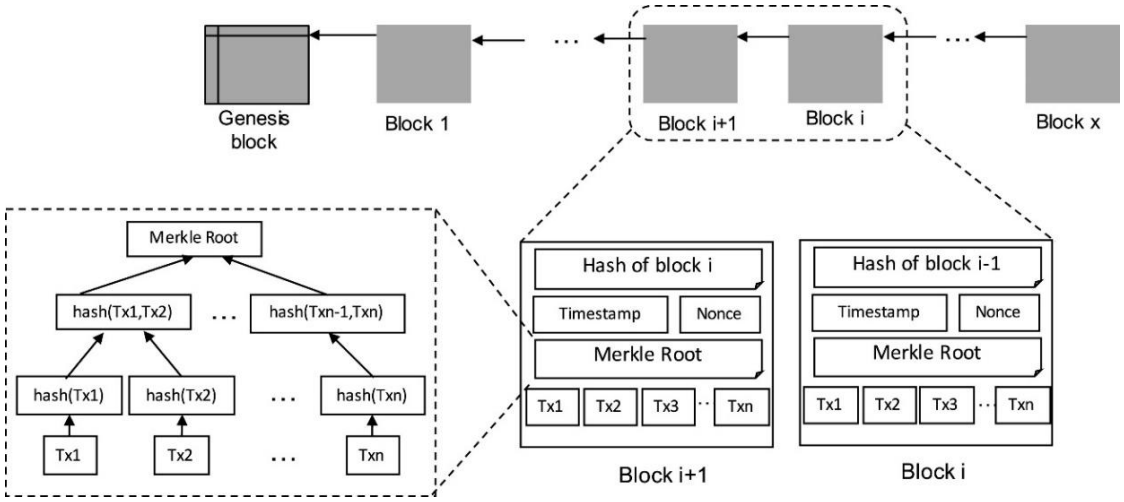


Figura 1.5. Estructura de un bloque
Fuente (Nasir et al., 2022)

Capa de red

La tecnología blockchain utiliza una red Peer-to-peer, donde todos los participantes de la red son tratados como iguales, esta red es la encargada de la comunicación, sincronización y distribución de la información para mantener actualizado el estado global de la red. Los participantes son denominados nodos, los cuales están divididos en dos grupos:

- **Nodo completo:** Este tipo de nodos también denominados nodos de minería, son los encargados de realizar el proceso de verificación y validación de las transacciones por lo cual mantienen una copia de todo el historial de transacciones. Además, son los encargados de definir las reglas de consenso para la validación. Estos nodos son la raíz de confiabilidad del flujo de información agregada a la blockchain de manera veraz y sin adulteraciones.
- **Nodo normal:** Considerado como nodo ligero, a diferencia del nodo completo, este nodo solo puede generar y enviar transacciones a la red para su validación por los nodos mineros, quienes se basan en protocolos de consenso, el más conocido Proof of work (prueba de trabajo). Además, se denominan ligeros debido a que los nodos mineros cumplen con los requisitos de capacidad de almacenamiento mayor a 200Gb ya que necesitan tener a disposición todas las transacciones y verificar su validez.

Capa de consenso

La capa de consenso hace referencia a una reunión, donde la mayoría de los participantes deben estar de acuerdo, para generar bloques o validar transacciones. También

es considerado un conjunto de reglas que deben ser cumplidas por todos los nodos para obtener la confiabilidad en la red. Como podemos observar en la figura 1.4 se muestra dos algoritmos de consenso, el primero Proof of work, este se basa en el poder computacional para resolver un problema matemático, otorgando el privilegio de crear un bloque y en resultado recibe una recompensa. El segundo, Proof of Stake se basa en la cantidad de capital que tiene un nodo, para ser considerado como nodo validador y generar nuevos bloques (Nasir et al., 2022).

Capa de presentación o aplicación

Es considerada como capa de comunicación con la blockchain por medio de una interfaz amigable para el usuario. Esta capa se divide en capa de aplicación y ejecución, la primera cuenta con elementos como interfaces, apis y scripts por los cuales el usuario puede interactuar con todas las funciones del contrato inteligente. La capa de ejecución guarda la lógica del negocio, donde se implementan las funciones a ejecutar, mediante los contratos inteligentes.

Flujo de trabajo de blockchain

En la figura 1.6 se muestra el flujo de trabajo de transacciones realizadas en una red blockchain, haciendo énfasis en la red Bitcoin la cual es una red pública que utiliza el consenso para validar la información. A continuación, se presenta el proceso de una transacción en una red blockchain basado en el artículo "Scalable blockchains — A systematic review" del autor Nasir (2022).

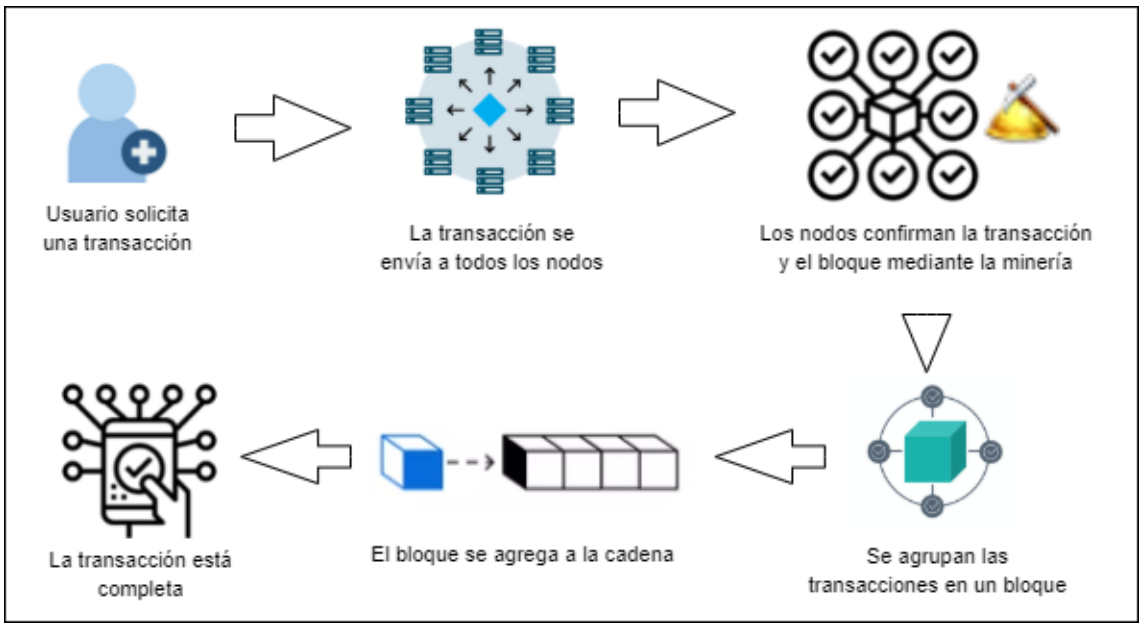


Figura 1.6. Proceso de una transacción en la blockchain
Fuente (Elaboración propia)

1. Un usuario realiza una transacción para enviar determinada cantidad de bitcoins, estas transacciones son anónimas debido al uso de una billetera digital donde se utiliza la clave publica similar a una cuenta bancaria.
2. La transacción generada es enviada a todos los nodos de la red P2P (peer-to-peer), quienes validan si la cuenta tiene fondos necesarios para ejecutar la transacción.
3. Los nodos mineros o completos validan y registran las transacciones mediante algoritmos de consenso, en el caso de bitcoin es proof of work (PoW), donde los mineros deben resolver un problema matemático para crear un nuevo bloque en la cadena con las transacciones válidas.
4. Todos los bloques tienen un límite de transacciones, por ende, las transacciones válidas deben esperar a que el bloque esté completo.
5. El bloque finalmente se agrega al final de la cadena de bloques de manera vinculada y de manera inmutable. En este punto se emite la recompensa a los nodos mineros por resolver el problema matemático.
6. La transacción está completa y el usuario receptor recibe la cantidad la cantidad de bitcoins.

1.2.3 Voto electrónico con blockchain

La tecnología blockchain tiene varias aplicaciones, uno de ellos es el voto electrónico, debido a que puede aportar características como: anonimato, privacidad, transparencia, descentralización y seguridad en la información, para obtener un sistema que no dependa de una entidad central, consiguiendo mayor confianza en los electores.

Existen muchos protocolos de voto electrónico usando blockchain para garantizar un proceso electoral más seguro, uno de ellos es el propuesto por Khan (2020) en el artículo “Investigating performance constraints for blockchain based secure e-voting system” donde expone el modelo de la figura 1.7.

Khan (2020) propone que cada votante debe contar con una billetera digital donde se le asigna una única ficha o token, el cual representa un voto con la finalidad de evitar el doble voto. Para sufragar los votantes deben estar registrados previamente para acceder al sistema. Los votantes envían una transacción a la dirección del candidato de su preferencia, la cual es contabilizada para posteriormente realizar el conteo respectivo. Al realizarse las transacciones con direcciones públicas, todo el proceso es anónimo y de manera transparente al utilizar una red pública donde todos los nodos de la red tienen acceso a la información y pueden considerarse como mineros para validar la veracidad de las transacciones (votos).

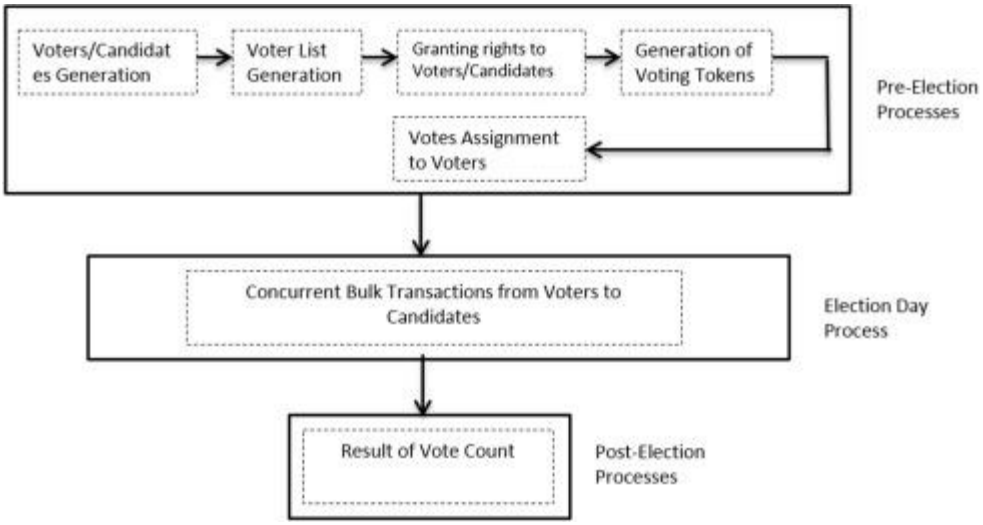


Figura 1.7. Proceso de votación con blockchain
Fuente (Kashif, Junaid, & Muhammad, 2020)

El voto electrónico con blockchain cubre varios requisitos para obtener mayor seguridad, por lo tanto, una plataforma que puede aportar mayor beneficio es Ethereum, debido a la implementación de contratos inteligentes, donde se definen las funciones que se ejecutan cuando se realiza una transacción. En el caso de las votaciones, se pueden definir las funciones para agregar candidatos, votantes o agregar votos a los candidatos para posteriormente realizar el respectivo conteo, mediante funciones que, una vez desplegado el contrato inteligente en una red blockchain, es inalterable. Estos contratos conllevan la lógica de negocio y se programan en base a sus necesidades para obtener una operación justa y sin intermediarios.

A continuación, se expone los componentes y beneficios de la tecnología blockchain, haciendo énfasis en el voto electrónico y su funcionamiento para obtener un sistema más seguro a diferencia del voto electrónico centralizado.

1.2.4 Beneficios de blockchain en el voto electrónico

Una de las características más importantes es la descentralización, es decir no necesita la participación de terceros o una entidad central, por lo cual aumenta la seguridad y confianza en un sistema de votación. Esta tecnología permite guardar la información de los votos en un registro inmutable y al ser una red pública todos los miembros de red pueden tener acceso y verificar la información, descartando la posibilidad de fraude.

La tecnología blockchain ha evolucionado desde su creación y ahora es denominada “Blockchain 3.0” debido a la implementación de juegos NFT, aplicaciones y finanzas descentralizadas, todo este ecosistema se basa en los contratos inteligentes, donde se

pueden especificar las condiciones que debe cumplir dicho acuerdo. Los contratos inteligentes toman un papel fundamental en las votaciones, debido al cumplimiento de condiciones de manera transparente e inalterable. Existen plataformas que permiten la creación de contratos inteligentes, la más conocida es Ethereum, sin embrago, por problemas de escalabilidad, se utilizará Polygon (cadena lateral) para implementar nuestro proyecto al ser una plataforma compatible con la máquina virtual de Ethereum (EVM), además, se considera que es una plataforma estable, la cual tiene una gran acogida por su flexibilidad, y se espera que tenga soporte por mucho tiempo.

Privacidad

Tomando como referencia al voto como una transacción, estas se pueden realizar mediante una billetera virtual o wallet donde a cada usuario posee una clave pública y privada. La clave publica funciona como un identificador único para cada persona, pero no revela la identidad y suele utilizarse para emitir las transacciones a un destinatario, por otro lado, la clave privada es la que permite el acceso a la wallet y su respectiva información, en este caso la privacidad se rompe si exponemos que la clave pública nos pertenece (K & Sree, 2021).

Según (Khan et al., 2020) mediante blockchain se logra el objetivo de mantener el voto secreto, debido a que cada votante utiliza la dirección de su billetera digital para transferir los votos a los candidatos

Transparencia

La transparencia es un principio fundamental tanto de la votación electrónica como en blockchain para aumentar la confianza del proceso. Este principio se cumple al utilizar una blockchain pública, debido a que la información es accesible para todos los nodos de la red, evitando manipulaciones y riegos de fraude, por lo tanto, permite auditar fácilmente el sistema. En un sistema de votaciones las funciones para el proceso de escrutinio, sufragio y resultados están descritas en un contrato inteligente, el cual es totalmente descentralizado e inmutable.

De acuerdo con (Khan et al., 2020) la tecnología blockchain reduce el riesgo de manipulación de información(votos) debido a que todo en la red blockchain se encuentra cifrado y el único que puede acceder a la transacción(voto) es la persona que lo emitió, todo esto sumado a los algoritmos de consenso. “El estado del proceso de votación se basa en un grupo de mineros de confianza que son responsables de aceptar una transacción de votación al agregarla a su bloque recién creado o simplemente pueden rechazar una transacción”(Khan et al., 2020).

Inmutabilidad

En una red donde todas las transacciones o votos realizados están distribuidos en todos los nodos, es imposible modificar o eliminar un registro una vez agregado a la blockchain debido a la transparencia de su red descentralizada. Su estructura se basa en el cifrado de cada bloque mediante un hash que hace referencia a una huella dactilar por lo tanto es única, cada bloque esta concatenado por un hash previo y cada hash de cada bloque hace referencia a su contenido, si el contenido cambia también cambia el hash, invalidando la cadena. Al ser una red descentralizada cada nodo tiene una copia exacta de la cadena de bloques, si llegará a alterarse un bloque se aplica una regla de consenso donde se atribuye valor a la cadena más larga y es remplazada por la corta, actualizando con información verificada por todos los miembros de la red (Zhang et al., 2020).

Seguridad

La seguridad de la blockchain depende principalmente de los mecanismos de consenso, que son las reglas que deben cumplir los nodos para crear bloques o validar transacciones, con el objetivo de mantener el funcionamiento correcto de la red. Además, debido a la criptografía, se garantiza la integridad de los datos en la cadena de bloques.

Descentralización y trazabilidad

Los usuarios no dependen de terceros que aprueben o autoricen las transacciones realizadas en una red blockchain gracias a la descentralización. En el caso de trazabilidad nos brinda la posibilidad de conocer todas las transacciones que ha realizado una cierta dirección, por lo cual, facilita la auditabilidad de un sistema, en este el de votación, evitando transacciones fraudulentas.

1.2.5 Algoritmos de consenso

El objetivo principal de los algoritmos de consenso es llegar a un acuerdo entre los nodos de la red para obtener el derecho de validar y procesar transacciones para posteriormente crear un bloque y añadirlo a la cadena de bloques, actualizando así el estado global de la blockchain. En un sistema de votación estos algoritmos nos ayudan a validar que los votos emitidos no sean fraudulentos. Existen dos tipos de algoritmos más usados por las plataformas de manera pública (Uzma, Mohd, & Zarina, 2021).

Proof of work (prueba de trabajo)

El algoritmo prueba de trabajo es usado por Bitcoin y Ethereum donde los participantes o nodos dedican gran parte de su energía computacional para resolver un acertijo y crear bloques por lo cual reciben una recompensa por el esfuerzo. Tiene mayor seguridad debido a la descentralización y aumenta dependiendo del número de participantes conectados a la red. En resumen, este proceso se realiza de la siguiente manera:

- Un determinado nodo envía una transacción a la red.
- Cualquier nodo de la red puede procesarla para construir un nuevo bloque.
- Los nodos deben resolver un acertijo o ejercicio matemático complejo, el primer nodo que lo logre puede recibir una recompensa y crear el blocque.

Este algoritmo se basa en la lealtad para recibir recompensas ya que si un nodo realiza transacciones fraudulentas pierde el derecho total a crear nuevos bloques y validar transacciones, resaltando que podría agregar la transacción, pero los demás miembros no la aprobarían o debería tener una mayoría en el consenso (Olawande & Darren, 2020).

Proof of Stake (prueba de participación)

Este algoritmo es una versión mejorada para solucionar los problemas de la prueba de trabajo, siendo más ecologista, donde no necesita un gran potencial computacional para agregar bloques, sino que los participantes deben tener una cierta cantidad de criptomonedas para obtener el derecho a validar transacciones. Esta garantía de fondos hace que el minero no realice transacciones fraudulentas para no comprometer sus fondos (Park, 2019).

A diferencia del anterior, los participantes son seleccionados de manera aleatoria, pero deben bloquear una cierta cantidad de dinero como garantía de confianza, este proceso se le llama “Staking” y los participantes se les denomina “Stake holders”. Si bien las recompensas no son en bitcoin, se obtienen las comisiones cobradas por la red a los usuarios que han realizado una transacción. Algunas plataformas utilizan este algoritmo entre ellas Neo, Stellar y próximamente Ethereum con la actualización de Ethereum 2.0, que actualmente se encuentra en una etapa experimental.

1.2.6 Contratos inteligentes

En un sistema de votación los contratos inteligentes hacen referencia a la lógica del sistema, en este caso autores como Dhulavvagol (2020) asocian los contratos como una urna donde se contabilizan los votos de manera automática sin la intervención de terceros, en base a las condiciones definidas antes de desplegar el contrato en la red blockchain. Los contratos

son fragmentos de código que generalmente responden a condiciones previamente programadas, para llevar a cabo un acuerdo sin la intervención de terceros de manera legitima (Yousif, Rajesh, Ting, & Joseph, 2021). Los contratos inteligentes se despliegan bajo la plataforma de Ethereum y son desarrollados mediante el lenguaje de programación solidity, un lenguaje basado en java y similar a JavaScript. Los contratos inteligentes tienen algunos beneficios como:

Transparencia

Uno de los beneficios significativos que provee los contratos inteligentes radica en la visibilidad de la lógica del contrato inteligente entre los miembros de la red o en el ecosistema de la cadena de bloques, a diferencia de las bases de datos centralizadas (Khan et al., 2020).

Ejecución Autónoma

La disponibilidad y ejecución del servicio es de manera automática debido a que no depende de un tercero centralizado, en este caso el estado de activación automático se define en el contrato inteligente pasando antes por la aprobación de los nodos de la red. Puede definirse cualquier condición como: transferencia de un pago o en el caso de la votación electrónica, control de un único voto por persona. (Hewa et al., 2021).

Precisión

Las condiciones dentro de un contrato inteligentes son inmutables como las cadenas de bloques, no se pueden cambiar una vez desplegadas con la aprobación de los miembros de la red. La ejecución es automática una vez que se cumplen las condiciones establecidas, sin la necesidad del factor humano, evitando errores y mejorando el grado de transparencia a través de una ejecución precisa y transparente (Hewa et al., 2021).

1.2.7 Desafíos de la tecnología blockchain

Uno de los principales desafíos es la escalabilidad, esta puede verse comprometida por la cantidad de usuarios que emitan el voto de manera simultánea al utilizar una red pública, donde los votos son considerados como transacciones en la blockchain. En solución a este problema utilizan protocolos de capa 2 o plataformas de blockchain privadas como HyperLedger Fabric para mejorar el tráfico de datos ya que una red privada o hibrida está determinada para un conjunto de usuarios exclusivos, donde la información permanece visible solo para la organización. Sin embargo, usar una red privada pierde la característica de descentralización, transformándola en una red parcialmente centralizada por la organización. (Uzma, Mohd, & Zarina, 2021).

Otro desafío que se presenta al usar blockchain es el costo de la implementación de los contratos inteligentes, así como también las transacciones que se realizan por medio de una red pública, en el caso de usar la plataforma Ethereum, el costo viene dado por ethers, la criptomoneda que maneja la plataforma. En este caso, el coste de transacción se mide en gas que es una cantidad fija de ethers la cual no se ve afectada por el aumento del valor de la criptomoneda.

Finalmente, tenemos uno de los desafíos que enfrentan todos los sistemas de votación electrónica, la aceptación y confianza del público en referencia a la participación de los electores. Si bien es cierto, blockchain puede acoplar sus características al sistema de votación para obtener mayor seguridad y confianza, pero es obsoleto si el público no tiene un grado de aceptación (Basilius, Moeljono, & Arya, 2021).

Soluciones de Escalabilidad en Ethereum capa 2

Ethereum es la segunda red más grande en el ecosistema blockchain y debido a su gran auge en aplicaciones descentralizadas (Dapps), Finanzas descentralizadas (Defi), NFT, existe un gran aumento en las transacciones lo que compromete su escalabilidad, dando como resultado altas tarifas de gas y un mayor tiempo de espera en la confirmación de las transacciones.

Como solución a esta problemática existen varios protocolos que se desarrollan en la capa 2. Por lo general existen dos capas en la red de Ethereum, la capa 1 en referencia a la red principal denominada mainnet y la capa 2, que son soluciones para mejorar la escalabilidad mediante el procesamiento de transacciones de manera exterior a la red principal, con la finalidad de disminuir la congestión y obtener un menor costo de transacción.

Cadenas laterales (Sidechains)

Las cadenas laterales o denominadas sidechains son exteriores a la cadena principal de Ethereum, por tanto, tienen sus propios algoritmos de consenso, su propio token y procesamiento de transacciones. Con el objetivo de obtener mayor seguridad existen sidechains llamadas Plasma chains, las cuales tienen sus raíces en la cadena principal para preservar su seguridad y debido a su propia moneda o token sus costos de transacción son relativamente bajos en comparación a Ethereum, permitiendo mayor velocidad en la confirmación de transacciones. Por lo general, estas cadenas cuentan con un puente a la cadena principal para transferir sus activos desde la capa 2 hacia la capa 1 o viceversa. Algunos ejemplos de estas cadenas son xDai, Polygon o Ronin (Amritraj, y otros, 2020).

Rollups

Denominados así porque agrupan una gran cantidad de transacciones en un lote y posteriormente se realiza una prueba a todo el lote en lugar de verificar cada transacción individualmente, para finalmente enviarlas a la cadena principal como una sola transacción, evitando grandes costos de transacción en la red principal. Sin embargo, existen dos tipos de rollups: optimistic rollups y ZK-rollups con diferentes características, pero mantenido la base de la solución rollups (Amritraj, y otros, 2020).

Por lo tanto, existen varias redes que tienen soluciones hibridas donde dependiendo de la red tienen diferentes mecanismos para mejorar la escalabilidad de la red principal. Además, siempre y cuando tengan compatibilidad con la EVM pueden implementarse Daaps con la misma estructura de Ethereum en diferentes redes como Binance Smart Chain, donde utiliza el protocolo de consenso de Proof of Stake (PoS) y su propia moneda BNB, siendo una red más rápida y menos costosa que puede aplicarse como una alternativa en una blockchain más accesible para los usuarios.

1.2.8 Plataformas blockchain que permiten contratos inteligentes

Ethereum es la primera red blockchain en implementar contratos inteligentes, sin embargo, existen varios proyectos que también los integran. En este apartado se exponen algunas plataformas a elegir para el desarrollo de nuestra prueba de concepto, con base en las siguientes características: escalabilidad, seguridad, descentralización, capacidad de procesar numerosas transacciones y bajos costos de transacción.

Ethereum

Es una plataforma que funciona de una manera completamente descentralizada y es capaz de procesar entre 10 a 15 transacciones por segundo, la cual carece de escalabilidad en términos de velocidad y rendimiento en comparación a Polygon o BSC. Ethereum implementa las denominadas Dapps (aplicaciones descentralizadas) mediante la Ethereum virtual machine (EVM). La EVM es el motor principal de la red de Ethereum, a diferencia de bitcoin que utiliza la tecnología blockchain para realizar las transacciones entre una cuenta a otra, la EVM permite la ejecución de programas denominados contratos inteligentes, mediante el lenguaje de programación solidity, facilitando su ejecución de manera autónoma (Coinbase, s.f).

La EVM ejecuta bytecode o lenguaje de máquina por lo cual, en primer lugar, se convierte solidity a código de operación (OP_CODES) y posteriormente a bytecode donde la EVM ejecuta las acciones establecidas en los contratos inteligentes. Ethereum usa tokens

ERC-20 y ERC-721 en su operación con los contratos donde hace uso del “Gas Price” como costo por los gastos computacionales. Todas las transacciones en la red de Ethereum tienen un costo denominado gas, este costo permite la validación de las transacciones mediante los nodos mineros, los cuales, tras validar la información correcta, reciben una recompensa, además hace imposible operaciones con bucles infinitos que puedan alterar el ecosistema de Ethereum (Shahzad & Crowcroft, 2019).

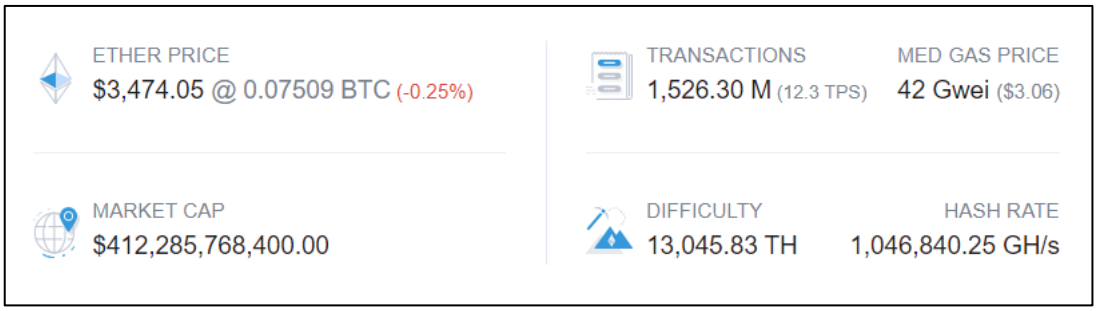


Figura 1.8. Resumen de la red Ethereum
Fuente (Coinbase, s.f)

Entre sus ventajas tenemos que es un sistema de código abierto por lo cual es libre a contribuciones en cuanto a mejoras por los desarrolladores de todo el mundo. Otra ventaja es su seguridad, basada en el algoritmo PoW. Además, cuenta con disponibilidad de la blockchain pública como privada y su criptomoneda nativa el Ether (Basilius, Moeljono, & Arya, 2021). Entre sus desventajas tenemos los elevados costos de transacción, alrededor de 3.06 dólares en transacciones simples tal y como se aprecia en la figura 1.8, cabe señalar que interactuar con los contratos inteligentes tiene un mayor costo. Otra desventaja es el tiempo de confirmación de las transacciones como resultado de la congestión en la red.

Binance Smart Chain (BSC)

BSC fue creada en 2020 y es considerada la segunda generación de blockchain que permite la ejecución de contratos inteligentes, a diferencia de la primera generación que tienen el propósito de producir el dinero digital como Bitcoin, Litecoin, Dogecoin, entre otras redes. BSC es una red perteneciente a Binance chain, la plataforma descentralizada más grande con el objetivo de realizar trading de manera rápida y descentralizada. Sin embargo, para la implementación de contratos inteligentes se desarrolla Binance Smart Chain, esta red cuenta con un algoritmo de consenso de autoridad de prueba de participación (PoSA), además de su notable escalabilidad, objetivo de competencia ante Ethereum, permitiendo manejar alrededor de 160 transacciones por segundo (Binance, 2021).

PoSA es similar a la prueba de participación (PoS) de Ethereum 2.0, donde los nodos validadores son seleccionados cada 24 horas, en base a la cantidad de BNB que poseen, siendo BNB la moneda de BSC. Además, cabe mencionar que la seguridad no solo se basa

en su algoritmo de consenso, sino que también en empresas como Certik y Peckshield que auditan periódicamente sus Daaps y tokens, para evitar incidentes y hackeos. Esta blockchain tiene compatibilidad con la máquina virtual de Ethereum (EVM), por tanto, hace posible la migración de Daaps desde Ethereum a BSC con la misma estructura, como también el soporte para las herramientas y Daaps de Ethereum (Binance, 2021).

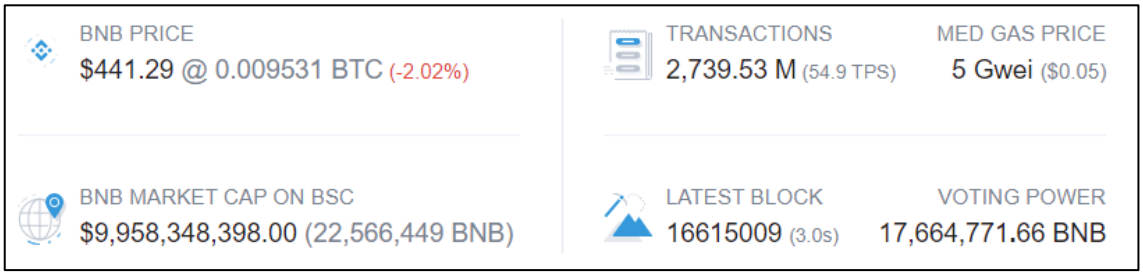


Figura 1.9. Resumen de la red BSC
Fuente (Binance, 2021)

Entre las ventajas destaca: tener su propio token BNB, por lo tanto, los costos de transacción en la red son más bajos, alrededor de 0.35 dólares tal y como se aprecia en la figura 1.9 y una mayor velocidad en la confirmación de transacciones. Entre sus desventajas encontramos: no es una red tan descentralizada, debido a que cuenta solo con 21 validadores que a diferencia de redes como Ethereum cuentan con una gran cantidad de nodos mineros.

Polygon (MATIC)

Polygon es una cadena lateral (sidechain), con el objetivo de solucionar los problemas de escalabilidad en Ethereum. Esta red utiliza el protocolo de consenso Proof of Stake (PoS) para validar las transacciones, siendo más rápido y eficiente que Proof of work (PoW), el cual es actualmente utilizado por Bitcoin y Ethereum.

En cuanto a la seguridad, esta red se beneficia de la estructura de Ethereum, utilizando sus nodos mineros para verificar de manera periódica la cadena de Polygon, a cambio de una tarifa. Además, es considerada semi descentralizada, debido a que cuenta con 100 nodos validadores a diferencia de Ethereum, con más de mil nodos mineros. Esta red es capaz de realizar 7000 transacciones por segundo y al igual que Ethereum, el precio por transacción se basa en el “Gas Price”, sin embargo, al poseer su propio token MATIC para efectuar transacciones, el precio de cada transacción esta entre 0.01 a 0.1 dólares tal y como se puede apreciar en la figura 1.10, debido a que cada token MATIC cuesta aproximadamente 1.60 dólares (Coinbase,s.f).

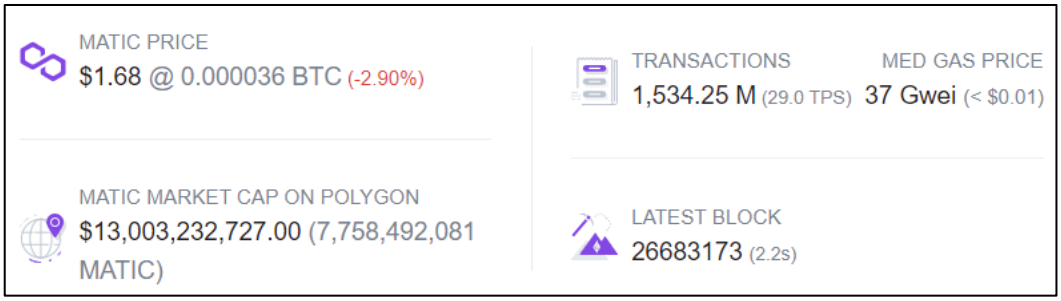


Figura 1.10. Resumen de la red Polygon
Fuente (Coinbase,s.f)

Una de las más importantes ventajas, es la compatibilidad con Ethereum virtual machine (EVM), la cual permite desplegar los contratos inteligentes de Ethereum en Polygon o viceversa. Además, al ser una cadena lateral, permite la comunicación bidireccional de las aplicaciones descentralizadas (Dapps) de Polygon con la blockchain de Ethereum. En tal sentido, se considera la mejor opción para nuestro sistema de votación el cual requiere un bajo costo en transacciones, seguridad y capacidad de procesar un gran número de transacciones.

1.2.9 Productos blockchain en el mercado

FollowMyVote

Es una organización que proporciona una solución al voto electrónico, utilizando la blockchain privada de Exonum y un esquema de firma ciega para obtener la privacidad de los electores. En primer lugar, el elector debe enviar información de su identidad (cédula o licencia de conducir) y esperar su validación por parte de la organización. Una vez verificada su información, el elector puede solicitar una boleta y enviarla, guardando su registro en la blockchain. Además, FollowMyVote permite realizar múltiples votos, considerando el último como legitimo. Finalmente, con su cuenta puede verificar la urna blockchain, para realizar una auditoría de los votos, conservando siempre el anonimato y la privacidad de los votos (Yang et al., 2020). (Di Francesco Maesa & Mori, 2020).

Agora

Es una empresa dedicada a la tecnología de votación con sus instalaciones en Suiza, cuenta con una blockchain personalizada por la propia empresa, llamada *Agora Bulletin Board,* considerada una blockchain pública con un mecanismo de consenso bizantino proactivo, que proporciona un alto rendimiento en la validación de transacciones. Agora protege la privacidad de los electores mediante el cifrado de ElGamal, además está vinculado a la blockchain de Bitcoin, en la cual almacena sus datos con la finalidad de obtener un alto nivel de descentralización e inmutabilidad, cabe destacar la accesibilidad que promete al

utilizar el sistema a través de cualquier dispositivo con acceso a internet de manera fácil y rápida. Finalmente, la empresa asegura el ahorro de costes en alrededor del 50% en el apartado de la administración electoral en comparación con los sistemas tradicionales existentes (Agora, s.f).

Polys

Es un proyecto de la organización Kaspersky y utiliza la blockchain de Exonum, su solución se basa en los contratos inteligentes para el proceso de votación, por lo tanto, cuenta con las características de: inmutabilidad, transparencia y auditabilidad. Polys se basa en un esquema de firma ciega para asegurar la privacidad y cuenta con una capa de servicio, encargada de la autenticación de electores. Los usuarios pueden utilizar el sistema desde el móvil o una computadora. Además, es un sistema modular que permite la flexibilidad en las papeletas (opción múltiple, única, referéndums), también cuenta con varios tipos de elecciones: municipales, organizaciones estudiantiles, partidos políticos o alguna encuesta presupuestaria (Polys, s.f.).

Voatz

Es una plataforma móvil especialmente para votaciones, basada en la tecnología blockchain y la tecnología biométrica para verificar la identidad del elector. Voatz utiliza Hyperledger como una blockchain de código abierto, asimismo proporciona una interfaz para los organizadores o administradores de la elección. Además, tiene las siguientes implementaciones: en 2018, Virginia Occidental usado por los militares, también, en 2017 para la elección del Senado de Tufts Community Union y finalmente en 2016 en Massachusetts en una convención estatal (Voatz, s.f).

CAPÍTULO 2

Desarrollo

El desarrollo del sistema de votación electrónica se realizó mediante la metodología Scrum como marco de desarrollo, la cual permite una gran flexibilidad a los cambios mediante sus iteraciones, dando como resultado un producto de calidad. Además, se hace uso de ***JavaScript*** como leguaje de programación por el lado del servidor y la librería ***React*** para la vista del cliente, juntamente con la librería ***Web3*** para la interacción con la blockchain.

2.1 Fase de Inicio Scrum

2.1.1 Definición de Roles

El primer paso es identificar el equipo de trabajo y las personas interesadas en el proceso, para la asignación de roles y responsabilidades. En la tabla 2.1 se presenta la definición de roles para el desarrollo de la aplicación informática.

Tabla 2.1: Asignación de roles Scrum

Nombre	Rol	Responsabilidad
PhD. Irving Reascos	Product Owner	Responsable de evaluar el cumplimiento de los requerimientos.
Sr. Alex Ipiales	Scrum Máster	Responsable de verificar el avance del desarrollo del sistema.
Sr. Alex Ipiales	Equipo Scrum	Encargado del desarrollo de la aplicación informática.
MSc. Mauricio Rea PhD. Iván García	Stakeholders	Apoyar y verificar el desarrollo de la aplicación informática

2.1.2 Definición del Product Backlog

En el product backlog o pila de producto, se definen las características o funcionalidades para el desarrollo del producto final, priorizando cada historia de usuario mediante la técnica ***T-Shirt Size – Effort Estimation***, esta técnica hace referencia a las tallas de camisetas como el esfuerzo que se requiere para realizar una tarea/historia de usuario, determinado por el tiempo (Bernhard, Markus, Mihai, & Wolfgang, 2010). A continuación, se presenta la estimación de esfuerzo en la tabla 2.2.

Tabla 2.2: Técnica T-Shirt Size

Estimación de esfuerzo	Talla de camiseta
10-20 horas	S
20-40 horas	M
40-60 horas	L

En la tabla 2.3 se presentan los requerimientos definidos con la prioridad, estimación y una descripción de las historias de usuario.

Tabla 2.3: Definición del Product Backlog

Código	Historias de Usuario	Estimación	Prioridad	Actividad
H1	Login administrador	S	Alta	El sistema debe permitir el inicio de sesión como administrador.
H2	Login elector	S	Alta	El sistema debe permitir el inicio de sesión como elector.
H3	Gestión de elecciones	M	Media	El sistema debe permitir la gestión de elecciones.
H4	Gestión de listas	M	Media	El sistema debe permitir la gestión de listas para una elección.
H5	Gestión de candidatos	M	Media	El sistema debe permitir la gestión de candidatos en una lista.
H6	Gestión de usuarios	M	Media	El sistema debe permitir la gestión de usuarios para el sufragio.
H7	Agregar listas a blockchain	L	Alta	El sistema debe permitir ingresar las listas a la blockchain en forma de transacciones.
H8	Efectuar voto	L	Alta	El sistema debe permitir efectuar el voto con la lista seleccionada.
H9	Mostrar Resultados	M	Media	El sistema debe mostrar los resultados de la elección mediante diferentes gráficas.

2.2 Fase de planificación y estimación

2.2.1 Definición de historias de usuario

En este apartado se busca identificar las necesidades del usuario en referencia a las funcionalidades del sistema mediante las historias de usuario.

Tabla 2.4: Historia de Usuario 1 - Login Administrador

HISTORIA DE USUARIO	
Numero: 1	**Usuario:** Administrador
Nombre de la historia: Login Administrador	
Prioridad: Alta	**Estimación:** S
Descripción: • Como administrador quiero que el sistema me permita iniciar sesión para realizar la gestión de elecciones, listas, candidatos y usuarios.	
Criterios de aceptación: • Mostrar un mensaje de error si el usuario ingresa de manera incorrecta los datos. • Los campos de usuario y contraseña son requeridos. • Si las credenciales son correctas, el usuario puede ingresar al módulo de administrador	

Tabla 2.5: Historia de Usuario 2 - Login Elector

HISTORIA DE USUARIO	
Numero: 2	**Usuario:** Elector
Nombre historia: Login elector	
Prioridad: Alta	**Estimación:** S
Descripción: • Como elector quiero que el sistema me permita iniciar sesión para posteriormente ejercer mi derecho al voto con una lista de mi preferencia.	
Criterios de aceptación: • Si las credenciales son correctas, ingresa al módulo de elector para sufragar. • Los campos de usuario y contraseña son requeridos. • Mostrar un mensaje si el usuario no está registrado.	

Tabla 2.6: Historia de Usuario 3 - Gestión de Elecciones

HISTORIA DE USUARIO	
Numero: 3	**Usuario:** Administrador
Nombre historia: Gestión de elecciones	
Prioridad: Alta	**Estimación:** M
Descripción: • Como administrador quiero que el sistema me permita realizar las actividades de gestión de elecciones tales como: creación, modificación y eliminación para posteriormente iniciar un proceso electoral.	
Criterios de aceptación: • No se puede crear una elección con la misma fecha de inicio y fecha de fin. • No se puede agregar elecciones con el mismo nombre. • No se pueden eliminar elecciones si contienen listas.	

Tabla 2.7: Historia de Usuario 4 - Gestión de listas

HISTORIA DE USUARIO	
Numero: 4	**Usuario:** Administrador
Nombre historia: Gestión de listas	
Prioridad: Alta	**Estimación:** M
Descripción: • Como administrador quiero que el sistema me permita realizar las actividades de gestión de listas, tales como: creación, modificación y eliminación, para posteriormente agregar candidatos.	
Criterios de aceptación: • No se pueden crear listas con el mismo nombre • El sistema solo puede cargar archivos con formato Excel para agregar varias listas. • No se pueden eliminar listas si contiene candidatos.	

Tabla 2.8: Historia de Usuario 5 - Gestión de candidatos

HISTORIA DE USUARIO	
Numero: 5	**Usuario:** Administrador
Nombre historia: Gestión de candidatos	
Prioridad: Alta	**Estimación:** M
Descripción: • Como administrador quiero que el sistema me permita realizar las actividades de gestión de candidatos, tales como: creación, modificación y eliminación. Además, quiero que el sistema me permita agregar diferentes cargos para los candidatos.	
Criterios de aceptación: • Mostrar los candidatos agregados • No se pueden agregar candidatos antes de agregar los cargos para los mismos.	

Tabla 2.9: Historia de Usuario 6 - Gestión de usuarios

HISTORIA DE USUARIO	
Numero: 6	**Usuario:** Administrador
Nombre historia: Gestión de usuarios	
Prioridad: Alta	**Estimación**: M
Descripción: • Como administrador quiero que el sistema me permita realizar las actividades de gestión de usuarios, tales como: creación, modificación y eliminación de los usuarios, para que puedan realizar el sufragio o en su defecto tener acceso al módulo de administrador.	
Criterios de aceptación: • No se puede agregar el mismo usuario más de una vez. • No se puede agregar usuarios con una cédula no válida. • La contraseña debe tener más de 6 caracteres. • El sistema debe proporcionar el formato a descargar con los campos del usuario. • El sistema solo permite cargar archivos en formato Excel para agregar varios usuarios.	

Tabla 2.10: Historia de Usuario 7 - Agregar listas a blockchain

HISTORIA DE USUARIO	
Numero: 7	**Usuario:** Administrador
Nombre historia: Agregar listas a blockchain	
Prioridad: Alta	**Estimación:** L
Descripción: • Como administrador quiero que el sistema me permita agregar las listas de una elección a la blockchain para obtener la inmutabilidad de los votos y el resultado.	
Criterios de aceptación: • El sistema permite agregar solo una vez las listas a la blockchain. • No se puede modificar o eliminar las listas una vez agregadas a la blockchain. • El sistema debe permitir elegir si se desea habilitar los votos nulos y blancos al proceso electoral.	

Tabla 2.11: Historia de Usuario 8 - Efectuar voto

HISTORIA DE USUARIO	
Numero: 8	**Usuario:** Elector
Nombre historia: Efectuar voto	
Prioridad: Alta	**Estimación:** L
Descripción: • Como elector quiero que el sistema me permita seleccionar una lista de mi preferencia para efectuar mi derecho al voto.	
Criterios de aceptación: • Mostrar las listas con los candidatos agregados previamente en una elección. • No se debe mostrar la vista para efectuar el voto antes de la fecha de inicio de la elección. • No se puede efectuar el voto más de una vez. • Se debe mostrar un mensaje al terminar de sufragar con el enlace del voto emitido en la blockchain.	

Tabla 2.12: Historia de Usuario 9 - Mostrar Resultados

HISTORIA DE USUARIO	
Numero: 9	**Usuario:** Administrador/ Elector
Nombre historia: Mostrar Resultados	
Prioridad: Alta	**Estimación:** M
Descripción: • Como administrador/elector quiero que el sistema me permita visualizar los resultados de una elección y conocer la lista ganadora con el número de votos y el porcentaje respectivo, sin la necesidad de iniciar sesión.	
Criterios de aceptación: • Los resultados deben ser mostrados con diferentes tipos de gráficos para mejorar la interpretación. • No se debe mostrar los resultados mientras la elección está en proceso.	

2.2.2 Planificación del proyecto

En la tabla 2.13 se presenta la asignación de las historias de usuario con cada sprint para el desarrollo del producto final, por lo tanto, cada sprint cuenta con una fecha de inicio y finalización basados en técnica de estimación *T-Shirt Size – Effort Estimation.*

Tabla 2.13: Planificación del proyecto por Sprints

ID	Historia de usuario	Estimación dificultad	Sprint	Fecha
1	Login/inicio de sesión del administrador	S	Sprint 1	(22/11/2021) al (06/12/2021)
2	Login/inicio de sesión del elector	S		
3	Gestión de elecciones	M	Sprint 2	(09/12/2021) al (23/12/2021)
4	Gestión de listas	M		
5	Gestión de candidatos	M	Sprint 3	(27/12/2021) al (10/01/2022)
6	Gestión de usuarios	M		
7	Agregar listas a blockchain	L	Sprint 4	(13/01/2022) al (03/02/2022)
8	Efectuar voto	L		
9	Mostrar Resultados	M	Sprint 5	(07/02/2022) al (26/02/2022)

2.3 Desarrollo del proyecto

Una vez especificado los roles, responsabilidades y requerimientos necesarios para el desarrollo del sistema, se continuó con el avance respectivo, comenzado con la ejecución de las iteraciones en el tiempo especificado. En cada sprint se realiza las revisiones del progreso del sistema con las funcionalidades requeridas antes de continuar con el siguiente sprint.

2.3.1 Tecnologías de desarrollo

A continuación, se presentan los conceptos de las tecnologías utilizadas en el desarrollo del sistema de votación, centrándose específicamente en las tecnologías de desarrollo blockchain.

Ganache

Es una blockchain local que nos permite realizar pruebas y desplegar nuestros contratos inteligentes. Además, tiene la posibilidad de enlazarse con Metamask, nuestra wallet. Su documentación se encuentra en el sitio web Truffle Suite (https://trufflesuite.com/ganache).

Truffle

Es un framework de desarrollo para Ethereum que permite crear, probar y desplegar contratos inteligentes en una red blockchain. Su documentación se encuentra en el sitio web Truffle Suite (https://trufflesuite.com).

Solidity

Es un lenguaje de alto nivel para programar contratos inteligentes para la red de Ethereum, su sintaxis es similar al lenguaje JavaScript. Su documentación se encuentra en el sitio web Solidity (https://docs.soliditylang.org/en/v0.8.13).

Web3

Es el medio de conexión entre una blockchian y un contrato inteligente, es decir, mediante web3 podemos ejecutar nuestros contratos y realizar transacciones. Su documentación se encuentra en el sitio web web3.js (https://web3js.readthedocs.io/en/v1.7.3)

Metamask

Es una billetera descentralizada que permite enviar o recibir activos digitales, además, es indispensable para enviar transacciones ya que cada transacción tiene un costo. Su documentación se encuentra en el sitio web Metamask (https://metamask.io).

Polygon

Es una plataforma de escalado Ethereum descentralizada que permite a los desarrolladores crear dApps escalables y fáciles de usar con tarifas de transacción bajas sin sacrificar nunca la seguridad. Su documentación se encuentra en el sitio web Polygon (https://polygon.technology).

MongoDB

Es una base de datos NoSQL orientado a documentos, por lo tanto, guarda los documentos en formato BSON, similar a JSON. Además, a diferencia de las bases de datos relaciones esta no necesita seguir un esquema. Su documentación se encuentra en el sitio web MongoDB (https://www.mongodb.com).

React

Es una librería basada en componentes que nos permite crear interfaces de usuario de forma ágil y versátil. Su documentación se encuentra en el sitio web React (https://es.reactjs.org).

Para el desarrollo del software utilizamos las herramientas que se pueden apreciar en la figura 2.1, se utiliza la librería ***React*** para la vista del cliente, denominada Front-end. Además, se utiliza ***Metamask*** para interactuar con la plataforma blockchain y la librería ***Web3*** que cumple el objetivo de conectarnos a las funciones de nuestro contrato inteligente. Adicional a ello, en la red ***Polygon*** se utiliza ***Solidity*** como lenguaje de programación para los contratos inteligentes y el *framework* ***Truffle***, que permite la compilación de estos en una red blockchain.

En el entorno de desarrollo se utiliza ***Ganache*** como una blockchain local y para el entorno de producción se utiliza la red ***Polygon***, una de las soluciones de escalabilidad para la capa 1 (Ethereum). Sin embargo, se pueden utilizar diferentes redes blockchain como: Binance Smart Chain, xDai o Avalanche, siempre y cuando tengan compatibilidad con la Ethereum virtual machine (EVM), debido a que comparten una estructura similar.

Finalmente, en el Back-end se utiliza ***Javascript*** como lenguaje de programación y ***Node*** como el entorno de ejecución. Además, se utiliza ***MongoBD*** la cual es una base de datos NoSQL. Sin embargo, para el almacenamiento de datos que incluyen información sensible o fácil de alterar en el proceso electoral, se utiliza la tecnología blockchain, considerando a la plataforma ***Polygon*** como la más accesible para esta prueba de concepto, debido a sus características estudiadas previamente.

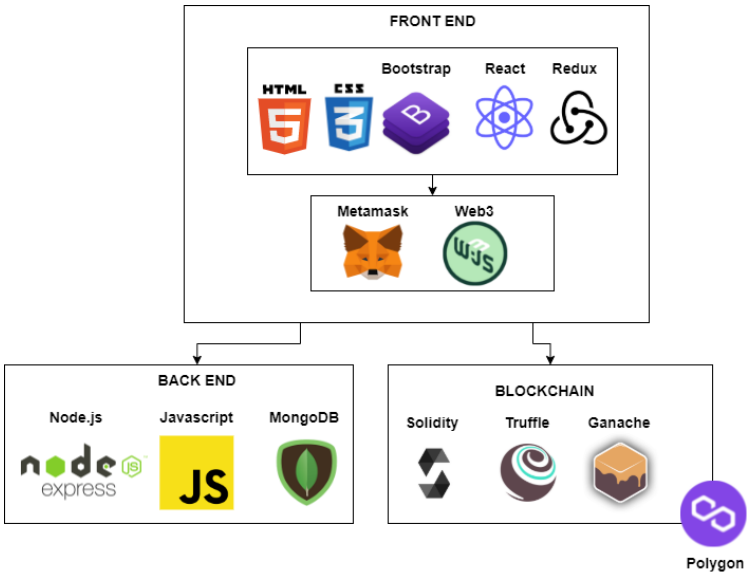


Figura 2.1. Tecnologías utilizadas en el sistema
Fuente: propia

2.3.2 Esquema de la aplicación

La aplicación web permite el inicio de sesión mediante el rol administrador y elector, el administrador puede realizar la gestión de elecciones, listas, candidatos y usuarios, mientras que el elector puede realizar el proceso de sufragio. Además, gracias a la tecnología blockchain permite el sufragio, escrutinio y resultados de manera descentralizada, inmutable y transparente mediante su trazabilidad, evitando la posibilidad de fraude.

En la figura 2.2 se muestra el diagrama de la aplicación desarrollada y la forma que interactúan sus componentes. Es decir, un usuario puede utilizar la aplicación web mediante un dispositivo conectado a internet, la aplicación utiliza la librería ***web3*** para interactuar con las funciones del contrato inteligente desplegado en la blockchain, además, nuestra billetera digital (***Metamask)*** nos permite aceptar o rechazar las transacciones de nuestro contrato inteligente y es un puente de conexión a nuestra red blockchain de ***Polygon*** para el almacenamiento de los votos y el proceso de escrutinio. Finalmente tenemos la base de datos de ***MongoBD*** donde se almacena la información de nuestro proceso electoral.

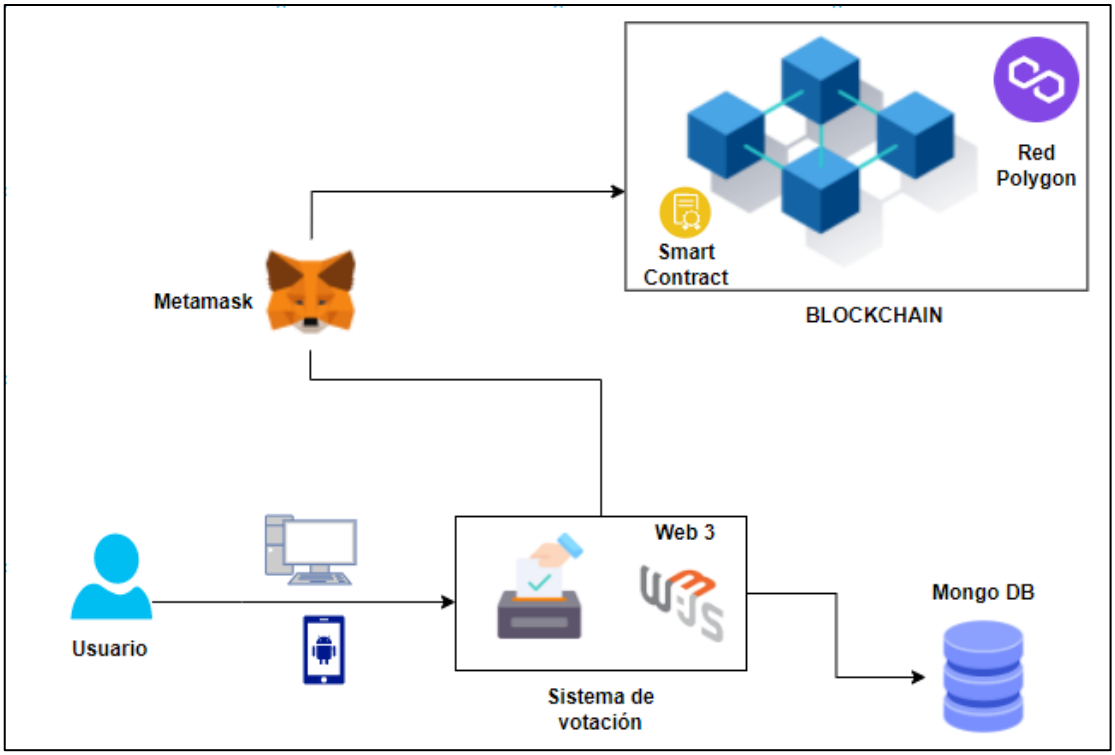


Figura 2.2. Diagrama de la aplicación
Fuente: propia

2.3.3 Planificación del sprint 1

En la tabla 2.14 se muestra el Sprint 1. Esta iteración tiene como objetivo el desarrollo de los roles del sistema (administrador/ elector), donde se obtiene el control de acceso a los diferentes módulos de cada rol.

Tabla 2.14: Sprint 1 – Desarrollo del login del administrador/elector

Sprint 1 **Fecha inicio:** (22/11/2021) **Fecha fin:** (06/12/2021)			
ID	**Historia de Usuario**	**Tarea**	**Horas**
1	Login/inicio de sesión del administrador	Preparación del entorno de desarrollo.	3
		Creación de un proyecto con Node.js.	2
		Creación de un proyecto con React.	2
		Creación de una colección(usuario) en la base de datos.	2
		Desarrollo de la vista para el login del administrador.	4
		Conexión con la base de datos.	3
		Desarrollo del método iniciar sesión.	4
		Encriptación de contraseña.	2
		Validación de campos requeridos.	2
		Comprobación de funcionalidad.	4
		Total	26
2	Login/Inicio de sesión del elector	Implementación de JSON web token para la autenticación.	4
		Creación del método iniciar sesión.	3
		Validación del formulario login.	2
		Creación del API REST para login.	2
		Creación de rutas públicas y privadas.	2
		Comprobación de funcionalidad.	4
		Total	13
	Reuniones	Planificación del sprint dos	4
		Revisión del sprint	2
		Retrospectiva del Sprint	2
		Total	8
		TOTAL	53

2.3.4 Ejecución del sprint 1

Para tener una visión más amplia de las funcionalidades que obtendrá el sistema, se opta por realizar los casos de uso con referencia en las historias de usuario, con el objetivo de describir las diferentes actividades que puede realizar un actor al interactuar con el sistema. En la figura 2.3 se observa todas las actividades que se pueden realizar al momento de ingresar al sistema de votación.

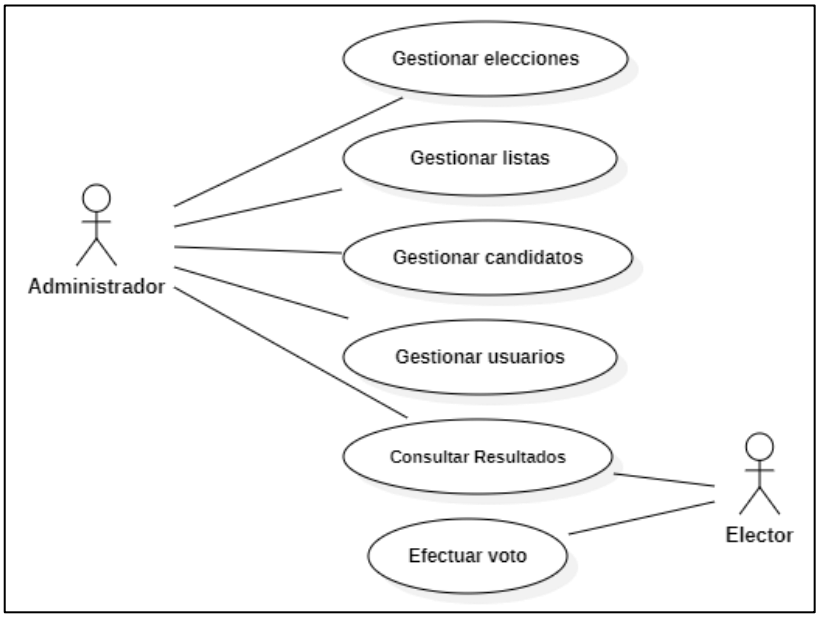


Figura 2.3. Caso de uso general del sistema

A continuación, se expone mediante imágenes el desarrollo de las tareas previamente planificadas en el Sprint 1.

Creación de la colección users en la base de datos.

En la figura 2.4 se muestra la colección ***users*** creada en la base de datos MongoDB, donde el atributo ***vote*** representa el estado de votación de cada usuario y por defecto inicia con el valor false cada vez que se genera un nuevo contrato inteligente.

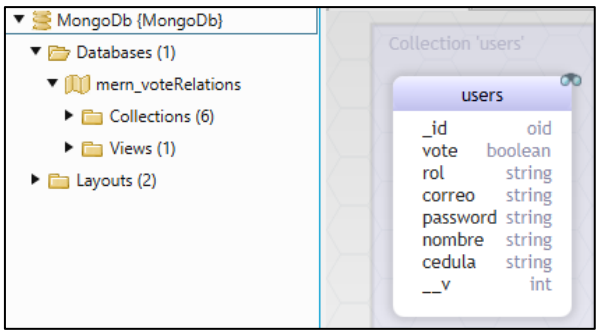


Figura 2.4. Colección de usuarios

Desarrollo de la vista para el login del administrador y elector

En la figura 2.5 se muestra la vista del login, la cual es usada por el rol de administrador y elector, restringiendo sus vistas en base al rol, en la figura 2.6 se puede apreciar sus respectivas validaciones al momento de iniciar sesión.

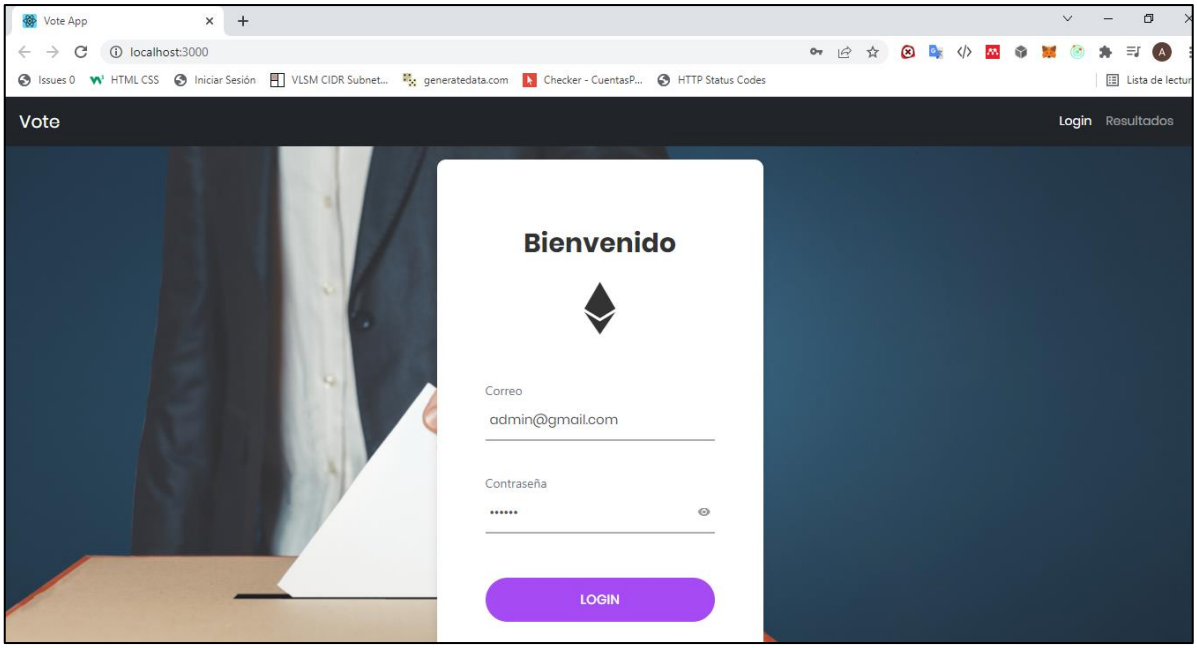


Figura 2.5. Vista del login

Figura 2.6. Validación de los datos en el login

2.3.5 Planificación del sprint 2

En la tabla 2.15 se muestra el Sprint 2, donde se cumplen las tareas para el módulo administrador, habilitando la gestión del proceso electoral: creación de elecciones y listas mediante una interfaz visual.

Tabla 2.15: Sprint 2 - Gestión de elecciones y listas

Sprint 2

Fecha inicio: (09/12/2021)

Fecha fin: (23/12/2021)

ID	Historia de Usuario	Tareas	Horas
3	Gestión de Elecciones	Creación de una colección(elección) en la base de datos.	2
		Creación del API REST para elecciones	3
		Creación del formulario para agregar o editar elecciones.	3
		Creación de la vista para listar elecciones.	4
		Desarrollo del método agregar elecciones.	2
		Desarrollo del método modificar elecciones.	2
		Desarrollo del método eliminar elecciones.	2
		Control de fechas ingresadas para la elección.	3
		Rutas de navegación.	3
		Comprobación de funcionalidad.	5
		Total	29
4	Gestión de Listas	Creación de una colección(lista) en la base de datos.	2
		Creación del API REST para listas	3
		Creación de la vista para las listas	4
		Desarrollo del método agregar	2
		Desarrollo del método modificar listas	2
		Desarrollo del método eliminar listas	2
		Almacenar imágenes de las listas en Cloudinary	4
		Permitir la carga de archivos Excel para agregar varias listas	4
		Creación de mensajes de notificación para el manejo de errores.	2
		Comprobación de funcionalidad	5
		Total	30
	Reuniones	Planificación del sprint tres	2
		Revisión del sprint	2
		Retrospectiva del Sprint	2
		Total	6
		TOTAL	65

2.3.6 Ejecución del sprint 2

En la figura 2.7 se muestra el diagrama de casos de uso para la gestión de elecciones, desde el punto de vista del administrador. Al ingresar al sistema, el administrador puede observar las elecciones existentes y de manera opcional puede crear, modificar o eliminar elecciones. Este diagrama hace referencia a la historia de usuario 3.

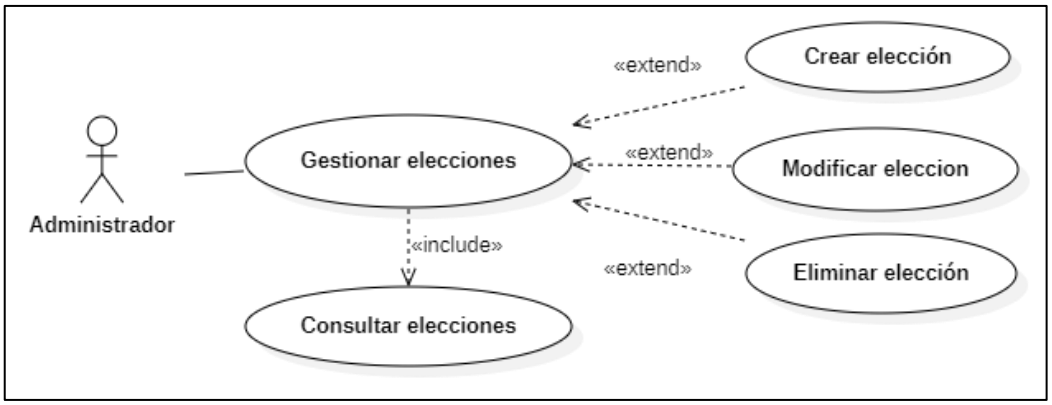


Figura 2.7. Caso de uso Gestión de elecciones

Al igual que el caso anterior, en la figura 2.8 se muestra el diagrama de casos de uso para la gestión de listas, donde el administrador puede observar las listas existentes y de manera opcional puede crear, modificar o eliminar listas. Sin embargo, antes de crear una lista es obligatorio, seleccionar una elección. Este diagrama hace referencia a la historia de usuario 4.

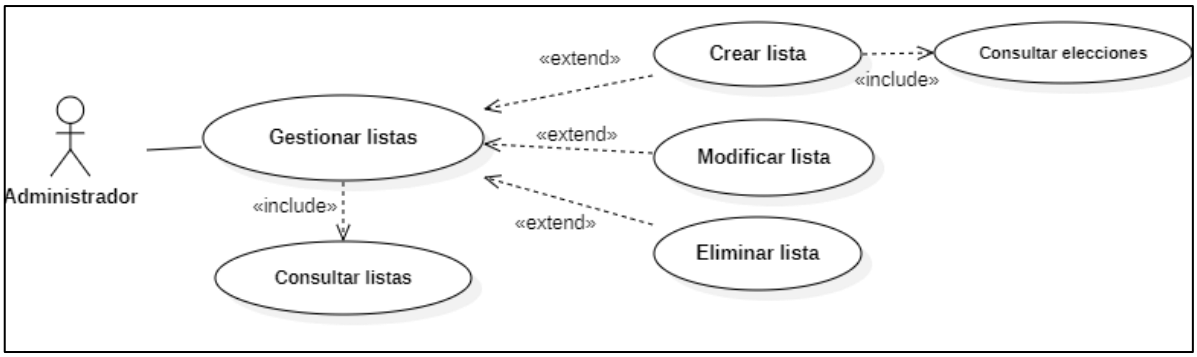


Figura 2.8. Caso de uso Gestión de listas

A continuación, se expone mediante imágenes el desarrollo de las tareas previamente planificadas en el Sprint 2.

Creación de la colección eleccions en la base de datos.

En la figura 2.9 se muestra la colección ***eleccions*** para gestionar las elecciones desde el módulo de administrador. Esta colección permitirá crear elecciones con un nombre,

descripción, fecha de inicio (start) y fecha de finalización (end) para posteriormente agregar sus respectivas listas de candidatos.

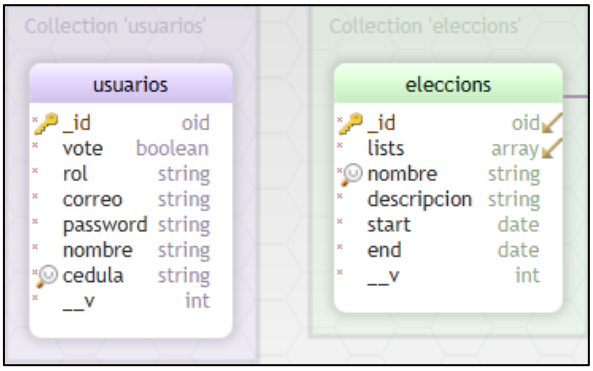


Figura 2.9. Colección de elecciones

Creación de la colección listas de candidatos en la base de datos.

El sistema permite realizar la gestión de listas por cada elección, por lo cual se crea una colección ***listas*** relacionada con la colección ***eleccions***. Esta colección permitirá crear listas de candidatos con un nombre, descripción, elección y un campo para determinar si se aceptan votos nulos y blancos en una elección (voteBN) para posteriormente agregar sus respectivos candidatos, figura 2.10.

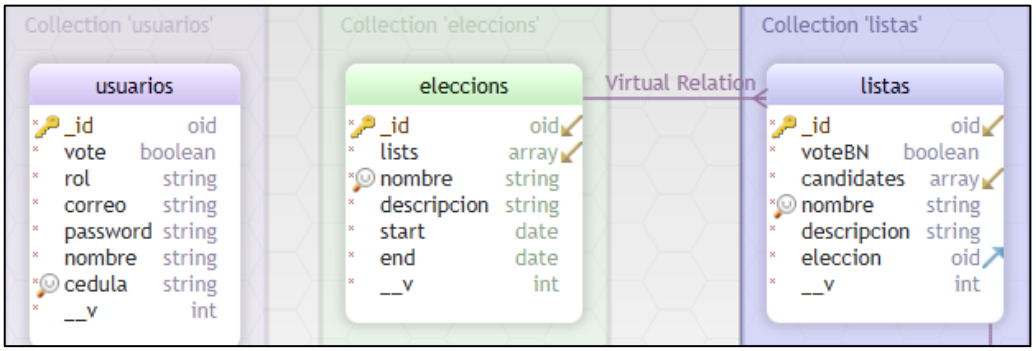


Figura 2.10. Colección de listas de candidatos

Creación de la vista elecciones

En la figura 2.11 se muestra la vista de elecciones con sus respectivas opciones para editar o eliminar. En el caso de la figura 2.13 se puede apreciar el formulario que se presenta al momento de crear o editar una elección. Además, se despliegan las advertencias antes de eliminar una elección, asimismo no se pueden eliminar elecciones mientras contengan listas de candidatos, figura 2.12.

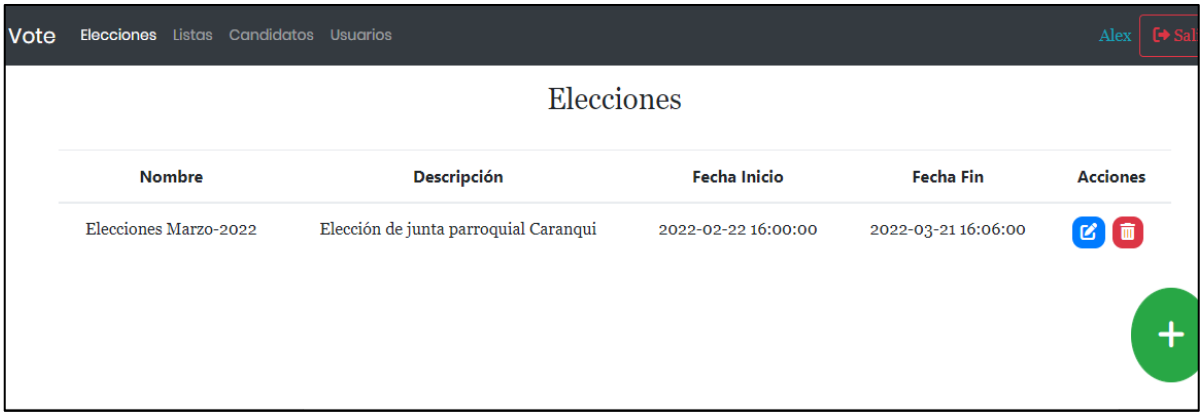


Figura 2.11. Vista de elecciones

Figura 2.12. Advertencias al eliminar una elección

Figura 2.13. Formulario para ingresar o editar elecciones

Creación de la vista Listas de candidatos

En la figura 2.14 se muestra la vista de listas de candidatos, con sus respectivas opciones para crear, editar o eliminar. Además, muestra la dirección del contrato inteligente

desplegado en la red Polygon, con esta dirección podemos verificar que no existe ninguna transacción antes de iniciar con el proceso electoral.

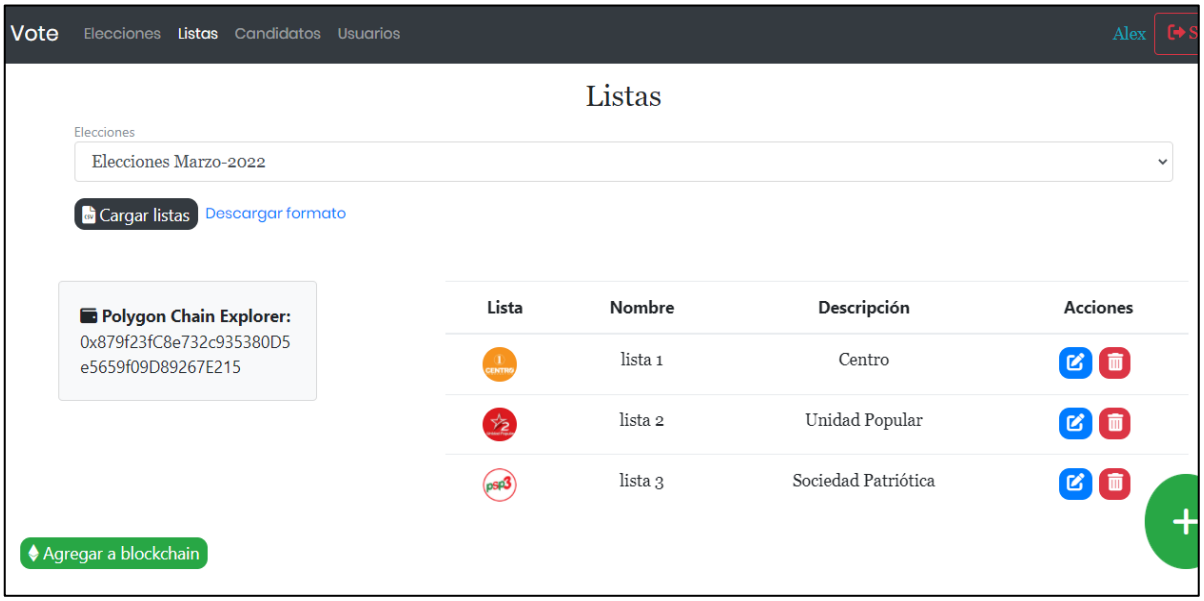


Figura 2.14. Vista listas

Cargar archivos Excel para agregar varias listas de candidatos.

En la figura 2.15 se muestra una ventana emergente, para seleccionar un archivo en formato Excel que contenga las listas que se desea agregar, posteriormente se pulsa el botón cargar listas para agregarlas a la base de datos.

Figura 2.15. Agregar listas desde un archivo Excel

Almacenar las imágenes de las listas de candidatos en Cloudinary

La figura 2.16 muestra el formulario para agregar o editar información de una lista, además se puede seleccionar una imagen que represente a la lista, estas imágenes son almacenadas en el servidor de Cloudinary. Finalmente, se despliegan las advertencias antes de eliminar una lista, asimismo no se pueden eliminar las listas mientras contengan candidatos, figura 2.17.

Figura 2.16. Formulario para agregar listas

Figura 2.17. Advertencias al eliminar una lista

2.3.7 Planificación del sprint 3

En la tabla 2.16 se muestra el Sprint 3, donde se cumplen las tareas para el módulo administrador, habilitando la gestión completa del proceso electoral con la gestión de candidatos y votantes mediante una interfaz visual, para posteriormente realizar el módulo de electores para su respectivo sufragio.

Tabla 2.16: Sprint 3 - Gestión candidatos y votantes

Sprint 3 **Fecha inicio:** (27/12/2021) **Fecha fin:** (10/01/2022)			
ID	**Historia de Usuario**	**Tarea**	**Horas**
		Creación de una colección(candidato) en la base de datos.	2
		Creación de formularios para agregar o editar candidatos.	3

		Creación del API REST para candidatos	3
		Creación de la vista para candidatos.	3
		Creación de la vista para los cargos de los candidatos.	2
5	Gestión de Candidatos	Método para agregar cargos y eliminar.	4
		Método para agregar candidatos.	2
		Método para modificar candidatos.	2
		Método para eliminar candidatos.	2
		Rutas de navegación	2
		Almacenar imágenes de los c en Cloudinary	4
		Comprobación de funcionalidad	4
		Total	31
		Creación de una colección(usuario) en la base de datos.	2
		Creación del API REST para usuarios	3
	Gestión	Creación de la vista para usuarios.	4
6	de	Implementación del método para validar cédulas de Ecuador.	2
	usuarios	Creación del método para agregar electores	2
		Creación del método para modificar electores	2
		Creación del método para eliminar electores	2
		Permitir la carga de archivos Excel para agregar varios electores.	3
		Desarrollo del método para limpiar el estado del voto de cada usuario, en un nuevo contrato inteligente.	3
		Comprobación de funcionalidad	4
		Total	27
		Planificación del sprint tres	2
	Reuniones	Revisión del sprint	2
		Retrospectiva del Sprint	2
		Total	6
		TOTAL	64

2.3.8 Ejecución del sprint 3

En la figura 2.18 se muestra el diagrama de casos de uso para la gestión de candidatos, desde el punto de vista del administrador. Al ingresar al sistema, el administrador puede observar los candidatos existentes y de manera opcional puede crear, modificar o eliminar candidatos. Sin embargo, para agregar candidatos, es obligatorio crear sus cargos y seleccionar una lista. Este diagrama hace referencia a la historia de usuario 5.

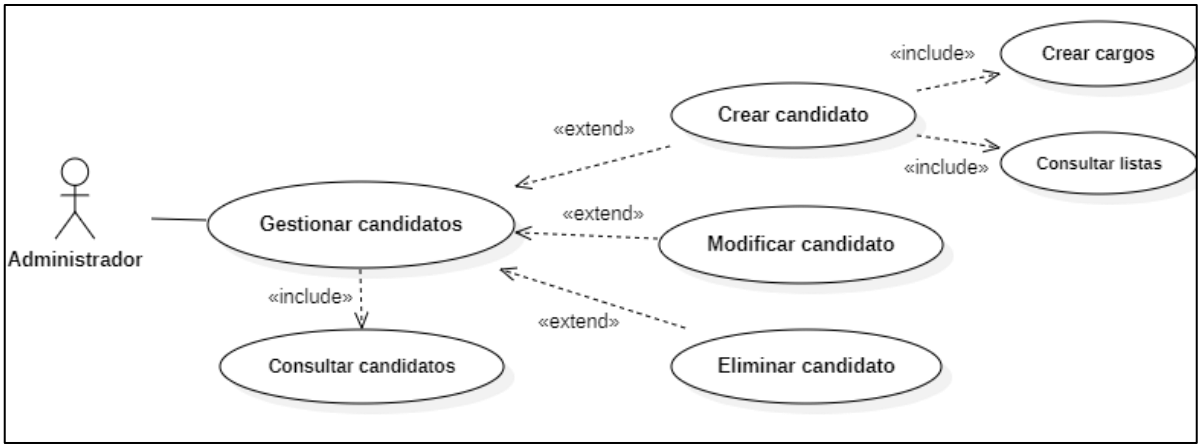


Figura 2.18. Caso de uso Gestión de candidatos

Al igual que el caso anterior, en la figura 2.19 se muestra el diagrama de casos de uso para la gestión de usuarios, donde el administrador puede observar los usuarios existentes y de manera opcional puede crear, modificar o eliminar usuarios. Sin embargo, antes de agregar un usuario es obligatorio, seleccionar un rol especifico. Este diagrama hace referencia a la historia de usuario 6.

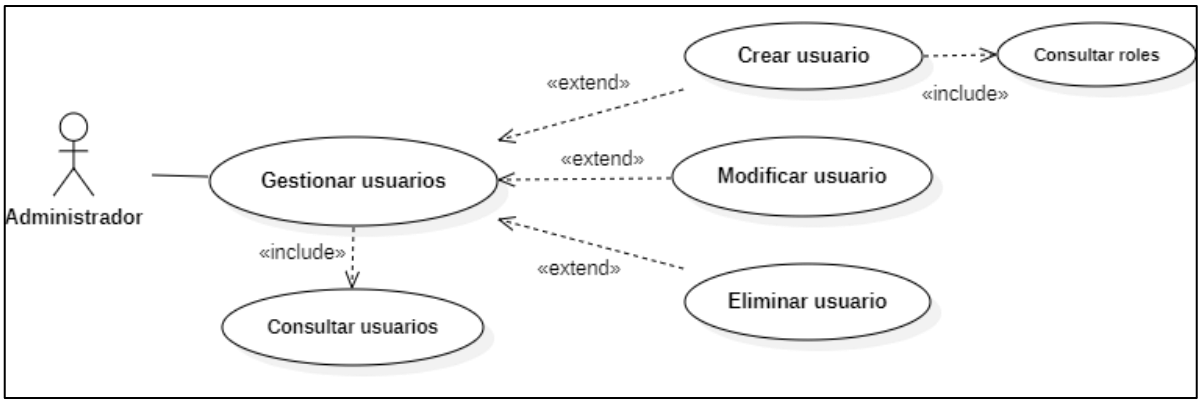


Figura 2.19. Caso de uso Gestión de usuarios

A continuación, se expone mediante imágenes el desarrollo de las tareas previamente planificadas en el Sprint 3.

Creación de la colección candidatos en la base de datos.

El sistema permite realizar la gestión de candidatos por cada lista, por lo cual se crea una colección ***candidatos*** relacionada con la colección ***listas*** tal y como se muestra en la figura 2.20. Esta colección permitirá agregar candidatos con un nombre, apellido, nombre de la lista, imagen y un cargo, los cuales son indispensables al momento del sufragio.

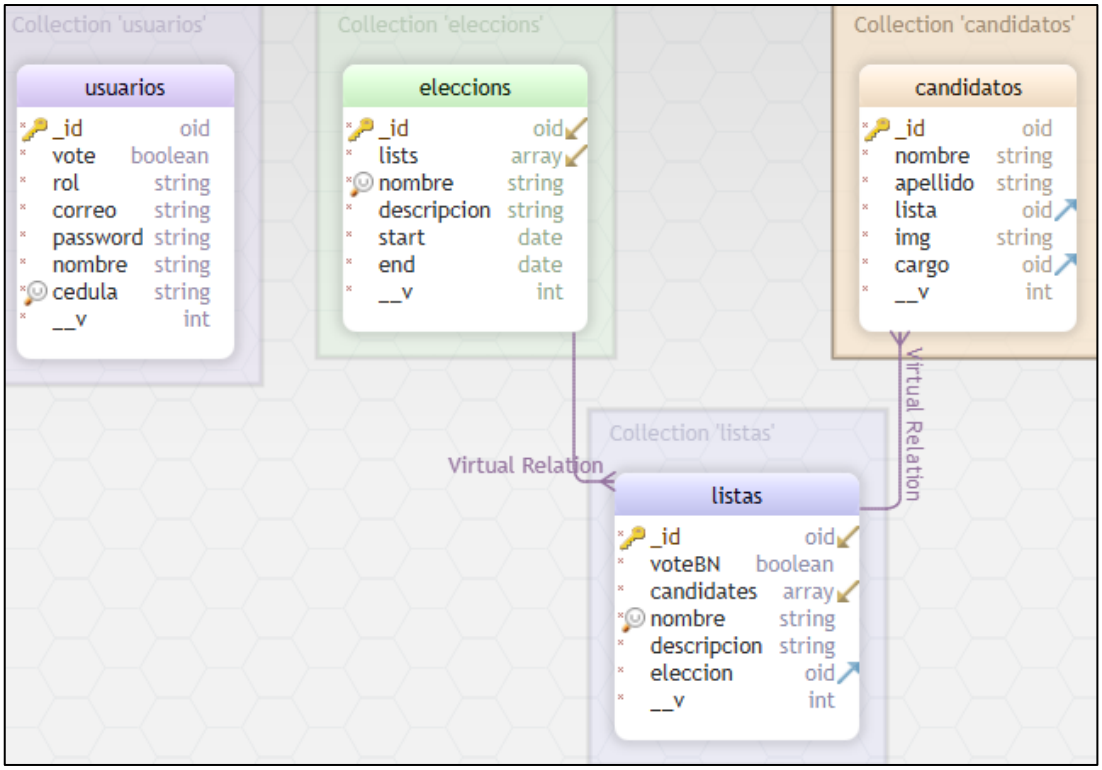


Figura 2.20. Colección de candidatos

Creación de la colección cargos en la base de datos.

Antes de agregar candidatos, es necesario crear sus cargos correspondientes, por lo cual se crea la colección ***cargos*** relacionada con la colección ***candidatos,*** donde tendrá como único atributo el nombre del cargo tal y como se muestra en la figura 2.21. Esta colección permitirá crear diferentes cargos como: presidente, vicepresidente, secretario, etc.

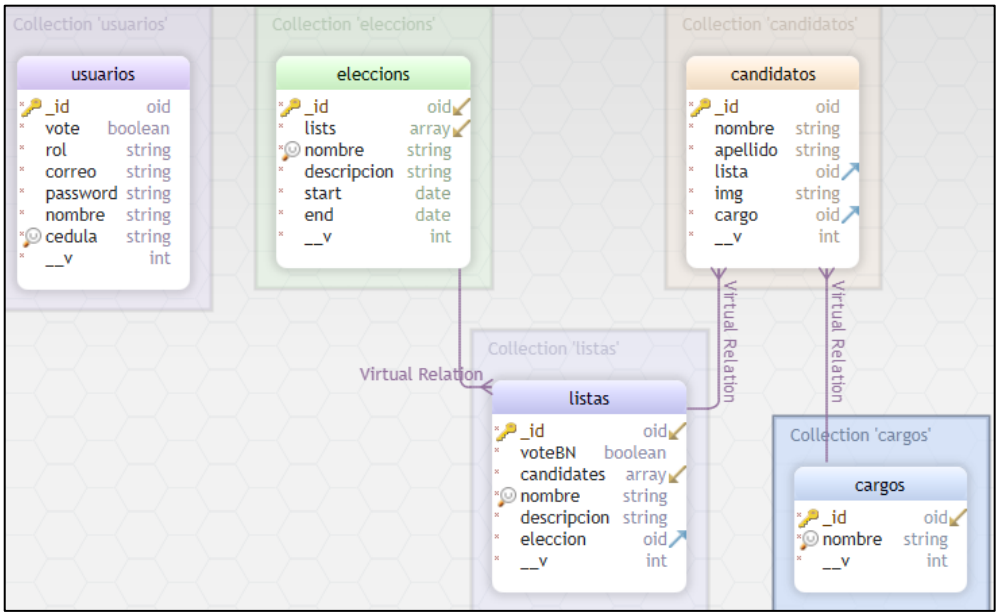


Figura 2.21. Colección de cargos

Creación de la vista candidatos

En la figura 2.22 se presenta la vista de candidatos con las listas de candidatos agregadas previamente, en esta vista se debe agregar los cargos que van a tener los candidatos, por lo tanto, si no existen cargos, no se pueden agregar candidatos y aparece un mensaje de error tal y como se muestra en la figura 2.24.

Figura 2.22. Vista de candidatos

Creación de cargos para candidatos

Se presenta una ventana emergente para agregar los cargos que sean necesarios antes de agregar los candidatos, en la figura 2.23 se muestra el campo para crear cargos, los mismo que se muestran en la tabla, con la única opción de eliminar debido a un único campo.

Figura 2.23. Creación de cargos para candidatos

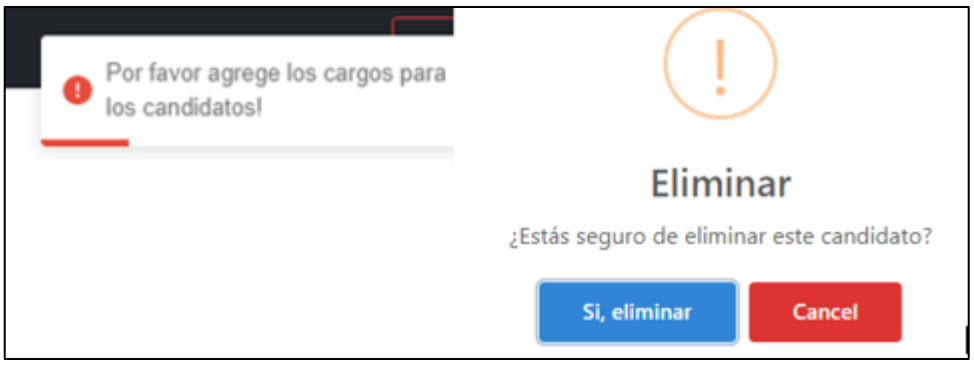


Figura 2.24. Advertencias al eliminar y agregar candidato

Creación de la vista usuarios

En la figura 2.25 se muestra la vista de usuarios con los diferentes roles, donde cada usuario elector tiene un estado del voto. Este estado cambia cuando el usuario sufraga. Además, esta vista cuenta con la carga de archivos en formato Excel para ingresar múltiples usuarios o en su defecto individualmente. Asimismo, se despliegan las advertencias antes de eliminar un usuario tal y como se muestra en la figura 2.26.

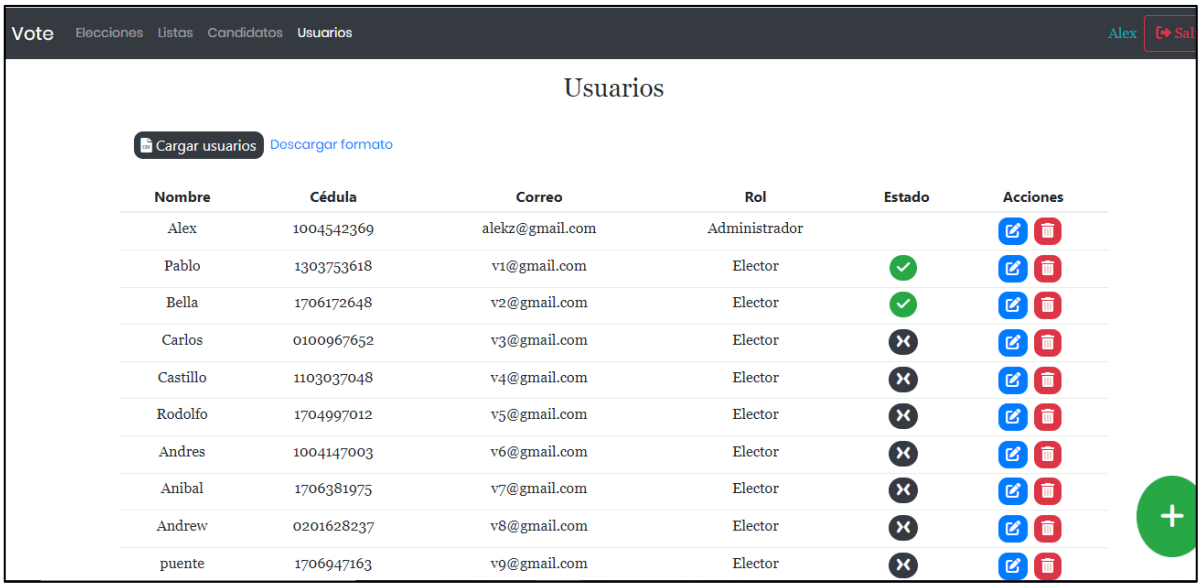


Figura 2.25. Vista usuarios

Figura 2.26. Validaciones de cédula y correo

2.3.9 Planificación del sprint 4

En la tabla 2.17 se muestra el Sprint 4 donde se cumplen las tareas para el módulo del elector, habilitando la función para el sufragio según la lista de su preferencia. Además, se configura el ambiente de trabajo para enviar las transacciones a la blockchain mediante contratos inteligentes.

Tabla 2.17: Sprint 4 - Efectuar voto

Sprint 4 **Fecha inicio:** (13/01/2022) **Fecha fin:** (03/02/2022)			
ID	**Historia de Usuario**	**Tarea**	**Horas**
7	Agregar listas a blockchain	Creación del Smart Contract	2
		Conexión con la librería web3.js	3
		Configuración de Ganache (blockchain local)	4
		Configuración de la billetera digital Metamask y conexión con Ganache	3
		Implementación del método enviar voto.	3
		Implementación del método, contar votos.	3
		Implementación del método, agregar listas.	3
		Implementación del método, obtener ganador.	2
		Implementación del método, resultados.	2
		Verificación de datos en la blockchain para agregar listas.	3
		Investigación de blockchains compatibles con la EVM.	3
		Búsqueda de faucets para obtener monedas digitales de prueba.	3
		Instalación y configuración del framework truffle.	3
		Creación de un nodo en Infura.	3
		Conexión a la blockchain de Ethereum con la red de pruebas de Rinkeby, BSC, Polygon.	5
		Despliegue del contrato inteligente en la blockchain.	2
		Método para agregar votos nulos y blancos	3
		Comprobación de funcionalidad	6
		Total	56
		Creación de la vista para la votación	4
		Control de acceso mediante la verificación de fecha de inicio y fecha fin de la elección.	2

8	Efectuar voto	Actualización del estado de voto de cada elector(true/false), si ya ha sufragado.	3
		Enviar la transacción(voto) a la blockchain.	3
		Recibir la url de la transacción generada por el elector.	3
		Comprobación de funcionalidad	5
		Total	20
	Reuniones	Planificación del sprint cinco	2
		Revisión del sprint	2
		Retrospectiva del Sprint	2
		Total	6
		TOTAL	82

2.3.10 Ejecución del sprint 4

En la figura 2.27 se muestra el diagrama de casos de uso para efectuar el voto desde el punto de vista del elector. Al ingresar al sistema, el elector puede observar las listas existentes y de manera opcional seleccionar la lista de su preferencia para posteriormente confirmar su voto. Este diagrama hace referencia a la historia de usuario 8.

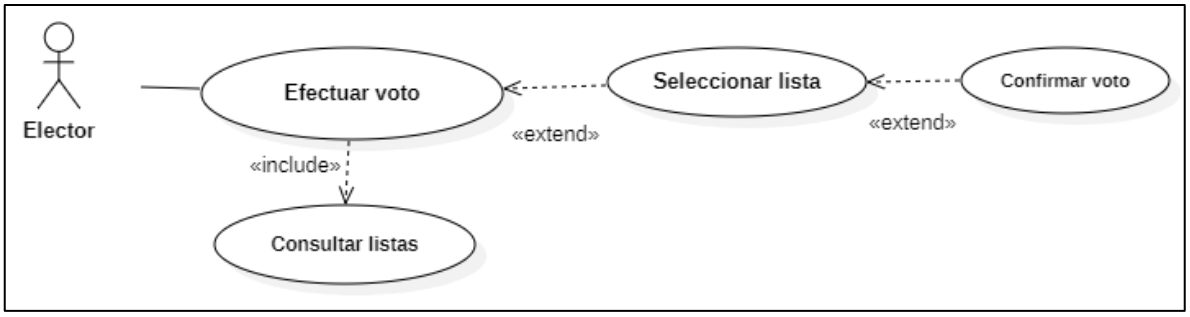


Figura 2.27. Caso de uso Efectuar voto

A continuación, se expone mediante imágenes el desarrollo de las tareas previamente planificadas en el Sprint 4.

Agregar listas de candidatos a la blockchain

En la figura 2.28 nos muestra las diferentes ventanas emergentes antes de agregar las listas de candidatos a la blockchain, la primera es un mensaje de advertencia antes de continuar con el proceso, si aceptamos la condición, nos aparece la segunda ventana donde podemos habilitar los votos nulos y blancos para el proceso electoral, los mismos que serán guardados en la blockchain para el sufragio.

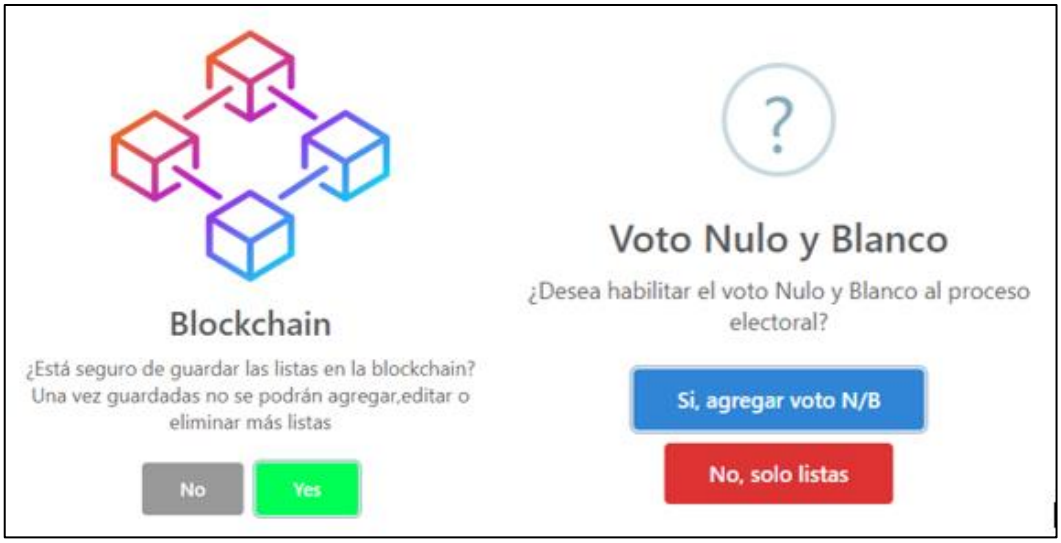


Figura 2.28. Habilitar voto nulo y blanco

En la figura 2.29 nos muestra la transacción y el costo para agregar las listas a la blockchain, generalmente se abre la billetera virtual para confirmar o rechazar la transacción donde podemos pagar un mayor costo y obtener una transacción más rápida o viceversa.

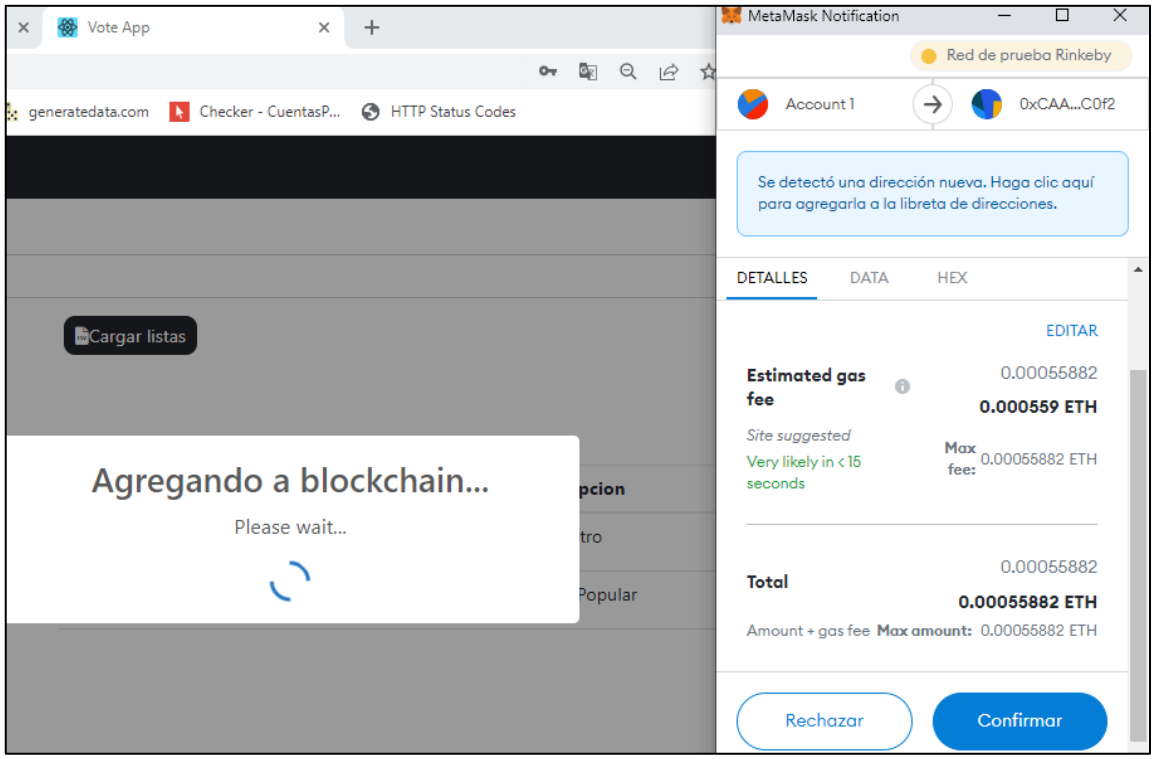


Figura 2.29. Agregar listas a blockchain con Metamask

Control de acceso mediante la verificación de fecha de inicio y fin de la elección

En la figura 2.30 nos muestra la verificación cuando la elección esta activa, en este caso nos muestra la elección inactiva debido a que ha terminado el proceso de votación o en su defecto, aún no inicia.

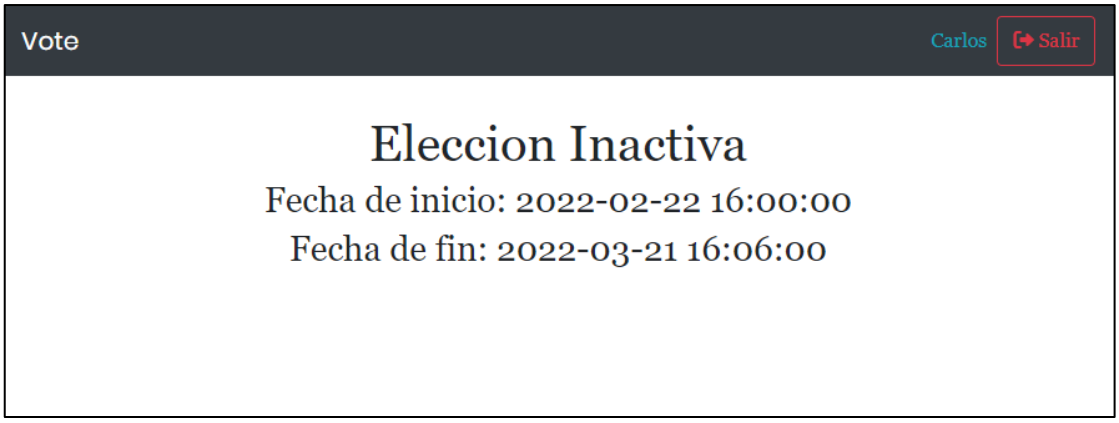


Figura 2.30. Verificación de elección activa

Creación de la vista para el sufragio

En la figura 2.31 se presentan todas las listas agregadas con sus respectivos candidatos, en este caso se muestran los votos nulos y blancos debido a que dependen del administrador para agregarlos a la elección al momento de agregar las listas a la blockchain.

Figura 2.31. Vista para el sufragio

Enviar el voto

En la figura 2.32 se aprecia que, al momento de elegir una lista, se abre la billetera de metamask, para aceptar la transacción del voto que posteriormente se almacenará en la blockchain, en forma de transacción de manera inmutable.

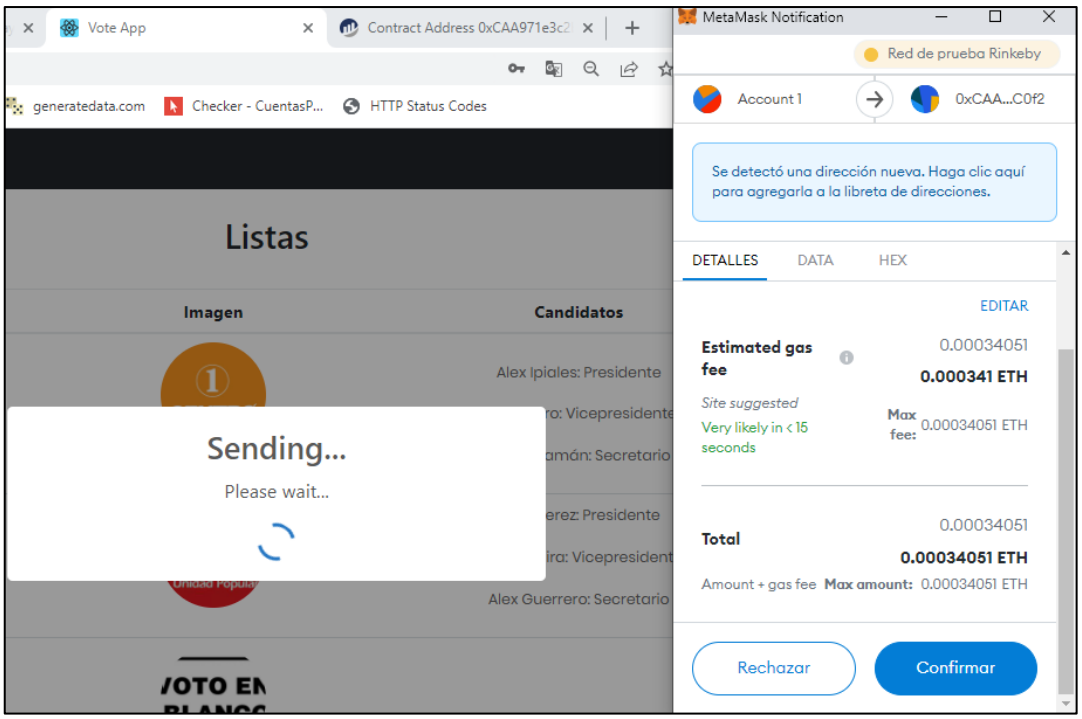


Figura 2.32. Enviar voto a la blockchain

Comprobar un único voto por cada usuario

Cada elector registrado previamente puede dar su voto solo por una sola vez, en el caso de volver a sufragar se despliegan advertencias donde nos indican si es su primera vez o es su segundo intento, dando resultados de error, como se muestra en la figura 2.33. Además, una vez realizado el voto se mostrará el enlace de la transacción y se podrá verificar la transacción en la red de Polygon tal y como se muestra en la figura 2.34.

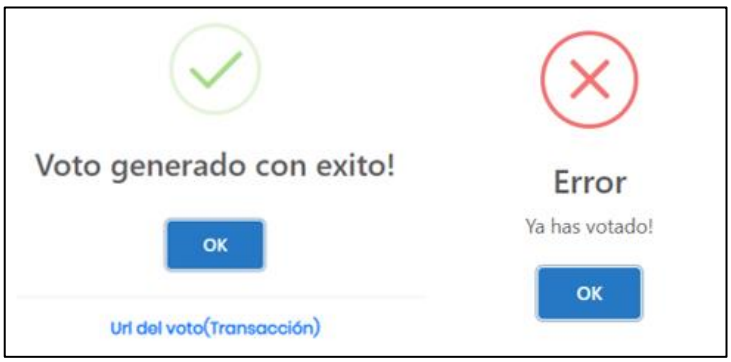


Figura 2.33. Verificación del voto

Figura 2.34. Voto en la blockchain

2.3.11 Planificación del sprint 5

En la tabla 2.18 se muestra el Sprint 5 donde se cumplen las tareas para visualizar el resultado de las elecciones tomando en cuenta la fecha de finalización, estos resultados están abiertos al público en general, siempre y cuando la elección haya concluido.

Tabla 2.18: Sprint 5 - Mostrar Resultados

Sprint 5 **Fecha inicio:** (07/02/2022) **Fecha fin:** (26/02/2022)			
ID	**Historia de Usuario**	**Tarea**	**Horas**
8	Mostrar Resultados	Rutas de navegación.	2
		Creación de la vista para resultados.	3
		Obtener resultados de la blockchain.	4
		Verificar si la elección ha finalizado.	3
		Mostrar resultados en la página principal.	2
		Implementación de diferentes gráficos para la interpretación de resultados.	4
		Comprobación de funcionalidad.	4
		Corrección de errores.	3
		Total	25

2.3.12 Ejecución del sprint 5

En la figura 2.35 se muestra el diagrama de casos de uso para consultar los resultados desde el punto de vista del administrador y elector. El usuario puede observar los resultados existentes y de manera opcional seleccionar o descargar el gráfico de su preferencia. Este diagrama hace referencia a la historia de usuario 9.

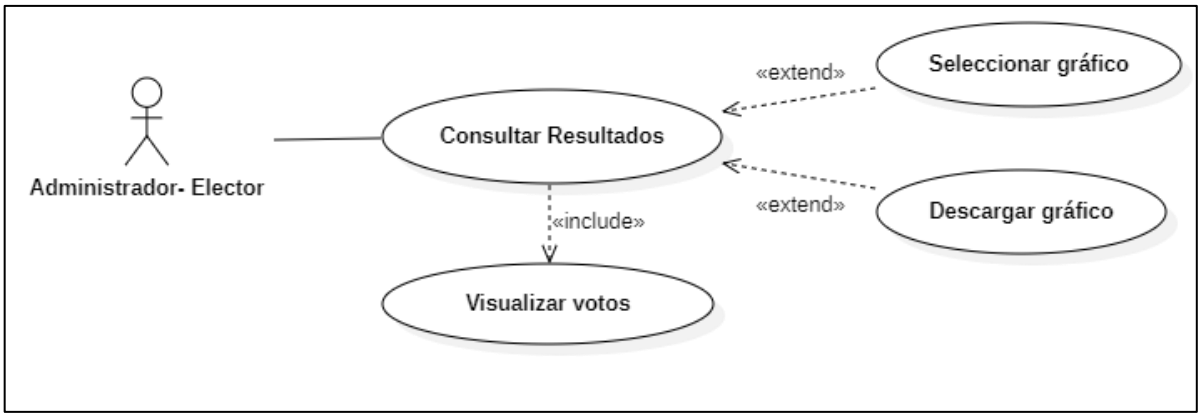


Figura 2.35. Consultar resultados de la elección

A continuación, se expone mediante imágenes el desarrollo de las tareas previamente planificadas en el Sprint 5.

Control de acceso mediante la verificación de fecha de inicio y fin de la elección

En la figura 2.36 nos muestra la verificación cuando la elección esta activa, en este caso nos muestra la elección en proceso debido a que aún no termina el proceso de votación o en su defecto, aún no inicia.

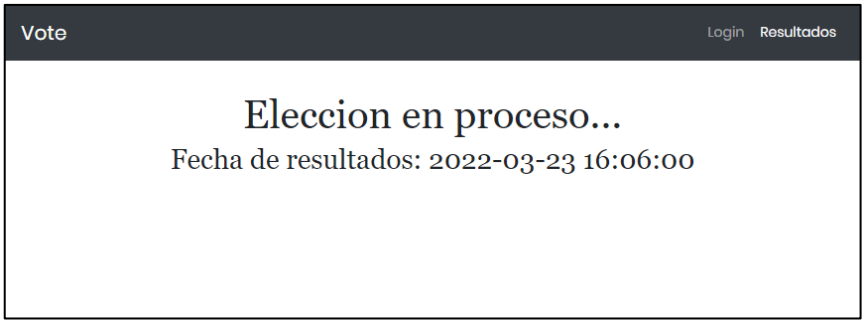


Figura 2.36. Verificación de elección finalizada

Creación de vista de Resultados

En la figura 2.37 se muestra los resultados obtenidos mediante gráficos que expresan el número de votos y el porcentaje, en esta vista el usuario puede elegir 3 tipos diferentes de graficas. Esta vista también muestra el ganador de la elección cuando pulsamos el botón obtener ganador.

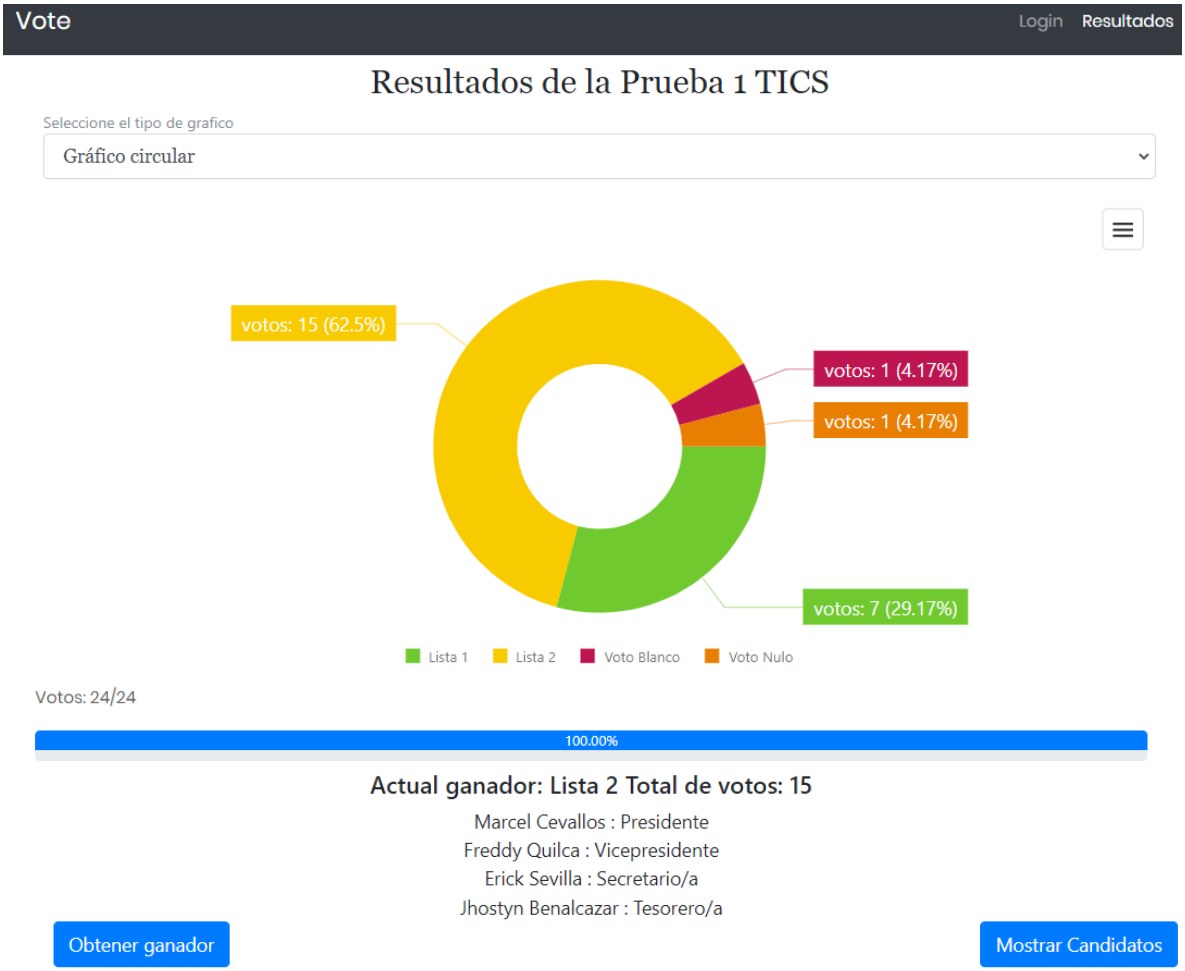


Figura 2.37. Vista de resultados

CAPÍTULO 3

Resultados

Este capítulo se centra en la validación del sistema de votación electrónica mediante el modelo de DeLone y McLean, el cual consiste en la relación de una serie de variables, agrupadas en 6 categorías: calidad del sistema, calidad de la información, calidad del servicio, intensión de uso, satisfacción del usuario e impactos netos. Esta validación se realizará en base a la interpretación y análisis de los resultados obtenidos mediante un cuestionario.

El objetivo principal de los SI (sistemas de información) es convertir los datos de una organización en información útil, que pueda ser usada en la toma de decisiones para el éxito de una organización, por ello un SI es considerada una fuente de oportunidad en el ámbito empresarial y de negocios. Asimismo, al invertir en un SI, se debe considerar los beneficios que puede aportar a la organización, en base a la solución de sus necesidades para obtener un mejor rendimiento y asegurar el retorno de la inversión.

La evolución de TI (tecnologías de la información) ha cambiado la forma de evaluar el éxito de un SI, sin embargo, esta medición sigue siendo simple porque se conservan elementos clave como: calidad del sistema, calidad de la información, el uso y los resultados, considerados como una base principal para el diagnóstico de éxito de los SI (DeLone & McLean, 2016).

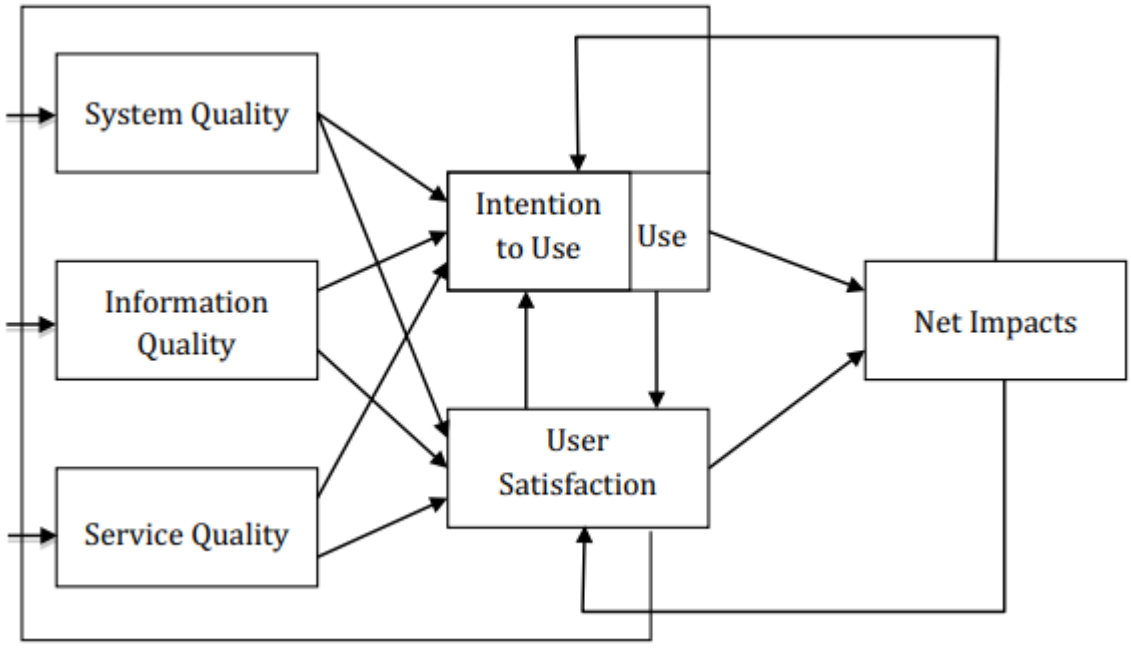


Figura 3.1. Modelo de éxito de DeLone and McLean
Adaptado de (DeLone & McLean, 2016).

En la figura 3.1 se muestra las variables de éxito individuales del modelo de DeLone & McLean, donde la calidad del sistema, calidad de la información y calidad del servicio influyen de manera directa en la intensión de uso y la satisfacción del usuario, por lo tanto, si el sistema presenta resultados positivos en las variables anteriormente descritas, influye en la intensión de uso por parte del usuario, en tal sentido, al interactuar con el sistema se puede obtener la satisfacción del usuario en relación al uso en un determinado tiempo. Es así como se consiguen los impactos netos, como el resultado de la relación entre todas las variables. Cabe destacar que, si el usuario no está satisfecho con el uso del sistema, no se obtendrán impactos netos que aporten de manera positiva a su objetivo.

3.1 Diseño del instrumento de medición

3.1.1 Planificación

En esta etapa se llevarán a cabo las siguientes actividades: definición de la unidad de análisis y elaboración del instrumento para la recolección de datos. La unidad de análisis utilizada fue: "Determinar el éxito de un sistema de información mediante el modelo de DeLone and McLean".

La siguiente actividad consiste en la elaboración de los instrumentos para la recolección de datos, por lo cual se diseñó 2 cuestionarios diferentes en base al cuestionario implementado por Adebowale (2017), donde utiliza las variables de éxito de los sistemas de información del modelo DeLone & McLean, el cual sirve para evaluar el éxito o eficacia de un SI.

A continuación, se presenta la matriz usada para definir las preguntas a usar en el cuestionario.

Tabla 3.1: Definición de las preguntas del cuestionario por dimensión

Modelo	Dimensiones	Variables	Ítems
Modelo de DeLone y McLean	Calidad del sistema	Facilidad de uso	1. ¿Es fácil de utilizar el sistema?
		Interactividad	2. ¿Encuentro la interfaz muy amigable e intuitiva?
		Flexibilidad	3. ¿Es fácil de acceder?
	Calidad de la información	Confiabilidad	4. ¿El sistema proporciona información confiable?
		Comprensión	5. ¿La información presentada es comprensible?
		Entendimiento	6. ¿El sistema proporciona diversas maneras de observar la información (gráficos)?

Calidad del servicio	Competencia técnica	7.	¿El soporte técnico brindado es útil logrando resolver alguna inquietud y/o inconveniente?
	Tiempo de respuesta	8.	¿El tiempo de respuesta cuando existe una inquietud y/o inconveniente es rápido y oportuno?
	Precisión	9.	¿El soporte técnico brinda ayuda comprensible y precisa?
	Confiabilidad	10.	¿En general, no tuve inconvenientes al usar la aplicación?
Intensión de uso	Extensión de uso	11.	¿Usar el sistema me permite sufragar más rápidamente?
	Motivación de uso	12.	¿Usar el sistema me permite votar desde cualquier lugar?
	Naturaleza de uso	13.	¿Usar el sistema me permite observar los resultados de manera rápida y precisa?
	Propósito de uso	14.	¿En general, yo encuentro útil usar el sistema para sufragar?
Satisfacción del usuario	Satisfacción del usuario	15.	¿Estoy satisfecho con el proceso de sufragio del sistema?
	Satisfacción total	16.	¿El sistema cumple con sus expectativas?
	Comodidad	17.	¿Se siente cómodo usando el sistema?
	Satisfacción de reportes	18.	¿Estoy satisfecho con la presentación dé resultados?
Impactos netos	Productividad	19.	¿El sistema me ahorra tiempo?
	Accesibilidad de resultados	20.	¿El sistema proporciona fácil acceso a la información de los resultados?
	Eficiencia	21.	¿El sistema me facilita el sufragio de manera rápida y fácil?

3.1.2 Recolección de datos

En esta etapa, se procedió a aplicar 2 cuestionarios a 28 estudiantes de la Universidad Técnica del Norte mediante la herramienta ***Microsoft Forms.*** El primero dirigido a los estudiantes que utilizaron el módulo de elector para sufragar, en este caso 23 estudiantes y el segundo para los estudiantes que utilizaron el módulo de administrador para la gestión de elecciones, en este caso 5 estudiantes.

Los cuestionarios tuvieron en promedio una duración de 2 minutos con 38 segundos para los electores y 3 minutos con 18 segundos para los administradores en ser finalizados.

3.1.3 Análisis de datos

Es importante mencionar que el análisis de datos solo será aplicado al cuestionario dirigido a los electores, debido a la cantidad de usuarios que lo respondieron: 23 estudiantes. Para el análisis de los datos se usó el software IBM SPSS statistics 26 para obtener la confiabilidad del instrumento mediante el alfa de Cronbach.

Alfa de Cronbach

En este apartado se va a medir la confiabilidad a través del coeficiente alfa de Cronbach del cuestionario realizado a los electores. "El coeficiente alfa de Cronbach es la forma más sencilla y conocida de medir la consistencia interna y es la primera aproximación a la validación del constructo de una escala" (Oviedo & Campo-Arias, 2005). Además, permite evaluar la magnitud de correlación existente entre los ítems del cuestionario y sus respuestas. En la tabla 3.2 se presenta el valor del coeficiente de Cronbach que determina el nivel de confiabilidad de una dimensión o todo un instrumento.

Tabla 3.2: Interpretación del coeficiente alfa de Cronbach
(Oviedo & Campo-Arias, 2005)

Coeficiente alfa	Interpretación
Inferior a 0.70	Confiabilidad baja
De 0.70 a 0.90	Confiabilidad aceptable
De 0.91 a 1.00	Existe redundancia o duplicación

En la tabla 3.3 se muestra la tabulación de resultados por cada ítem del cuestionario realizado a los estudiantes que utilizaron el sistema para sufragar. En esta tabla, las columnas representan las preguntas del cuestionario (P) y las filas representan los estudiantes (E). Las respuestas son de escala tipo Likert con un valor de 1 a 5, totalmente desacuerdo (1), en desacuerdo (2), no estoy seguro (3), de acuerdo (4) y totalmente de acuerdo (5).

Tabla 3.3: Matriz de datos - resultados del cuestionario

Sujeto	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21
E1	5	3	5	5	4	3	3	3	3	5	5	5	3	5	5	5	5	4	5	4	5
E2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
E3	5	3	5	3	3	3	5	4	4	5	5	5	4	5	5	5	5	3	5	5	5
E4	5	4	5	5	5	5	4	4	4	5	5	4	5	5	5	5	5	4	5	5	5
E5	5	4	5	5	5	5	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5
E6	5	4	4	5	5	5	5	4	5	4	5	5	5	5	5	5	4	5	5	5	5
E7	4	4	4	5	5	5	4	4	4	4	5	5	5	5	5	4	4	4	5	4	4
E8	4	5	5	3	4	5	5	5	5	5	5	4	4	4	5	4	5	4	4	4	4

E9	5	4	4	4	4	5	4	3	4	5	5	5	5	5	5	4	4	3	5	4	5
E10	5	4	4	5	5	5	4	3	4	4	4	4	5	4	5	4	4	4	4	4	5
E11	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4	4
E12	5	4	5	5	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5
E13	5	3	5	5	4	5	3	3	3	3	5	5	5	5	5	4	4	3	5	5	5
E14	5	3	5	2	5	5	3	3	3	5	5	5	5	5	5	5	4	3	5	5	5
E15	5	3	5	3	3	4	4	4	4	5	5	5	4	4	3	4	4	3	4	4	4
E16	4	4	4	4	3	5	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4
E17	5	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	4	4	5
E18	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	5	5	5
E19	4	2	5	4	4	4	4	4	5	4	5	5	3	5	4	4	4	3	5	3	4
E20	5	4	5	4	3	4	4	3	4	5	5	5	5	4	4	4	5	4	5	5	5
E21	5	4	5	4	5	5	4	5	5	5	5	5	5	5	5	5	4	5	5	5	5
E22	5	4	5	2	3	5	4	4	4	4	5	5	5	4	3	3	3	4	4	5	5
E23	5	4	5	4	5	5	4	4	4	4	4	4	4	5	4	4	5	5	4	5	5

En base a los resultados obtenidos del cuestionario se pudo determinar el coeficiente de Cronbach con ayuda del software IBM SPSS statistics 26. En la tabla 3.5 se puede apreciar de forma general los resultados de todas las dimensiones, además, en la tabla 3.4 se presenta el coeficiente total, considerando las 21 preguntas del cuestionario realizado a 23 estudiantes, los cuales utilizaron el sistema para sufragar en una elección.

Tabla 3.4: Coeficiente total de fiabilidad

Alfa de Cronbach	**N° de elementos**
,794	21

Tabla 3.5: Resultados del Alfa de Cronbach
Fuente: Obtenido de software IBM SPSS statistics 26

Variable	**Ítems**	**Media de escala si el elemento se ha suprimido**	**Varianza de escala si el elemento se ha suprimido**	**Correlación total de elementos corregida**	**Alfa de Cronbach si el elemento se ha suprimido**
Calidad del sistema	Ítem 1	87,6957	30,767	,311	,788
	Ítem 2	88,6522	30,237	,293	,789
	Ítem 3	87,7826	32,360	,001	,802
Calidad de la información	Ítem 4	88,3043	28,494	,317	,792
	Ítem 5	88,1739	27,150	,583	,768
	Ítem 6	87,8261	30,241	,265	,791

Calidad del servicio	Ítem 7	88,3478	31,146	,183	,794
	Ítem 8	88,3913	30,158	,235	,794
	Ítem 9	88,2174	29,905	,321	,787
	Ítem 10	87,9130	30,901	,206	,793
Intensión de uso	Ítem 11	87,5652	31,439	,236	,791
	Ítem 12	87,6957	31,494	,170	,794
	Ítem 13	87,8696	28,755	,479	,777
	Ítem 14	87,7391	29,474	,549	,777
Satisfacción del usuario	Ítem 15	87,8261	27,877	,614	,768
	Ítem 16	88,0435	28,680	,588	,772
	Ítem 17	88,0435	29,953	,372	,784
	Ítem 18	88,3913	27,794	,549	,772
Beneficios obtenidos	Ítem 19	87,7391	30,474	,354	,786
	Ítem 20	87,9130	29,901	,364	,785
	Ítem 21	87,6957	30,403	,383	,785

Interpretación

En la tabla 3.4 se puede observar que el alfa de Cronbach corresponde a 0.794, por lo tanto, según Oviedo & Campo (2005) nos brinda una clasificación de “confiabilidad aceptable”, esto quiere decir que la consistencia interna de todo el instrumento es aceptable para su aplicación. Además, el “Alfa de Cronbach si el elemento se ha suprimido” nos permite evidenciar que al suprimir el ítem 3 se puede mejorar el coeficiente, pasando de 0.794 a 0.802 en un próximo cuestionario, estos ítems no solo deben eliminarse, sino que también pueden mejorarse, convirtiéndose en ítems más comprensibles para el usuario y mejorando su puntuación.

3.2 Presentación de resultados

3.2.1 Análisis del perfil de los encuestados

En este apartado se presenta el perfil de los encuestados, considerando únicamente el sexo y la edad de los 28 estudiantes que utilizaron el sistema desarrollado.

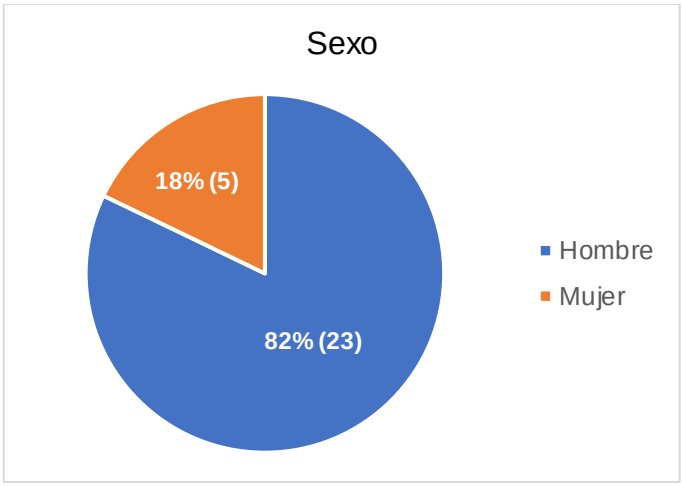


Figura 3.2. Género de los encuestados

En la figura 3.2 se puede apreciar el género de los encuestados, donde la mayoría de los usuarios que utilizaron el sistema son hombres, representando el 82% y el 18% eran mujeres.

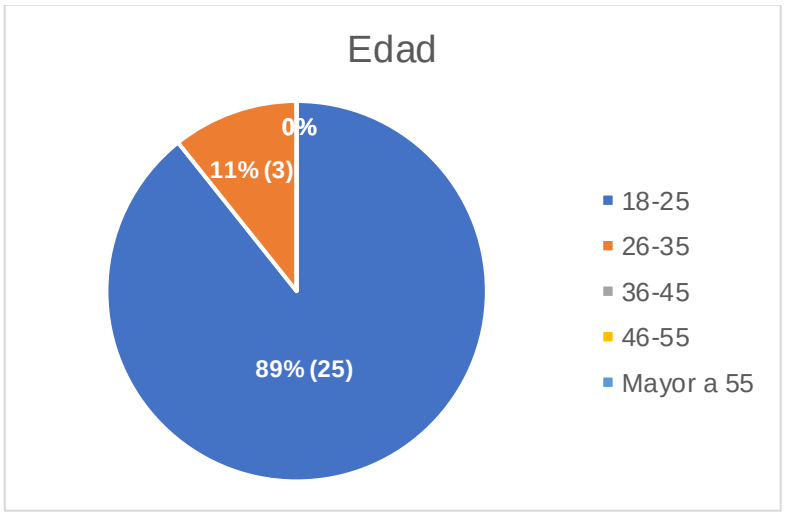


Figura 3.3. Edad de los encuestados

En el cuestionario realizado participaron estudiantes universitarios, por lo tanto, el rango de edad se concentró en los 18 a 25 años, representando el 89% y un 11% con un rango de edad entre los 26 a 35 años.

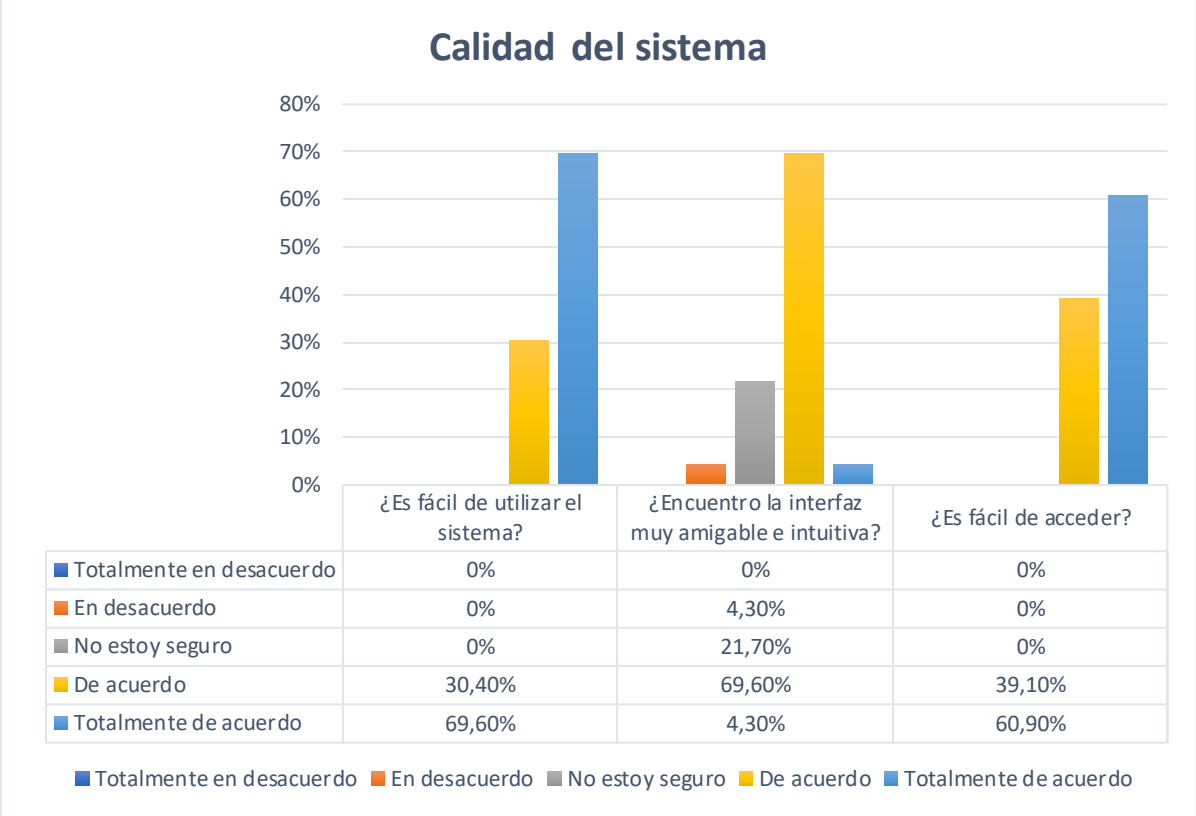
3.2.2 Variables del modelo de DeLone y McLean (cuestionario para electores)

En este apartado se presenta los resultados del cuestionario dirigido a los 23 electores que utilizaron el sistema para sufragar, estos resultados se basan en las dimensiones del modelo de DeLone y McLean. Las respuestas son de escala tipo Likert con un valor de 1 a 5, donde 1 corresponde a un total desacuerdo o inconformidad y 5 corresponde a una completa aceptación por parte del usuario.

A continuación, se expone las dimensiones del modelo de DeLone y McLean de manera más detallada con su respectiva interpretación de los resultados obtenidos.

Calidad del Sistema

La calidad del sistema es una característica que incluye medidas normalmente centradas en aspectos de usabilidad y rendimiento del sistema, por lo tanto, se debe tomó en cuenta las siguientes medidas: facilidad de uso, tiempo de respuesta y la interactividad con el usuario.



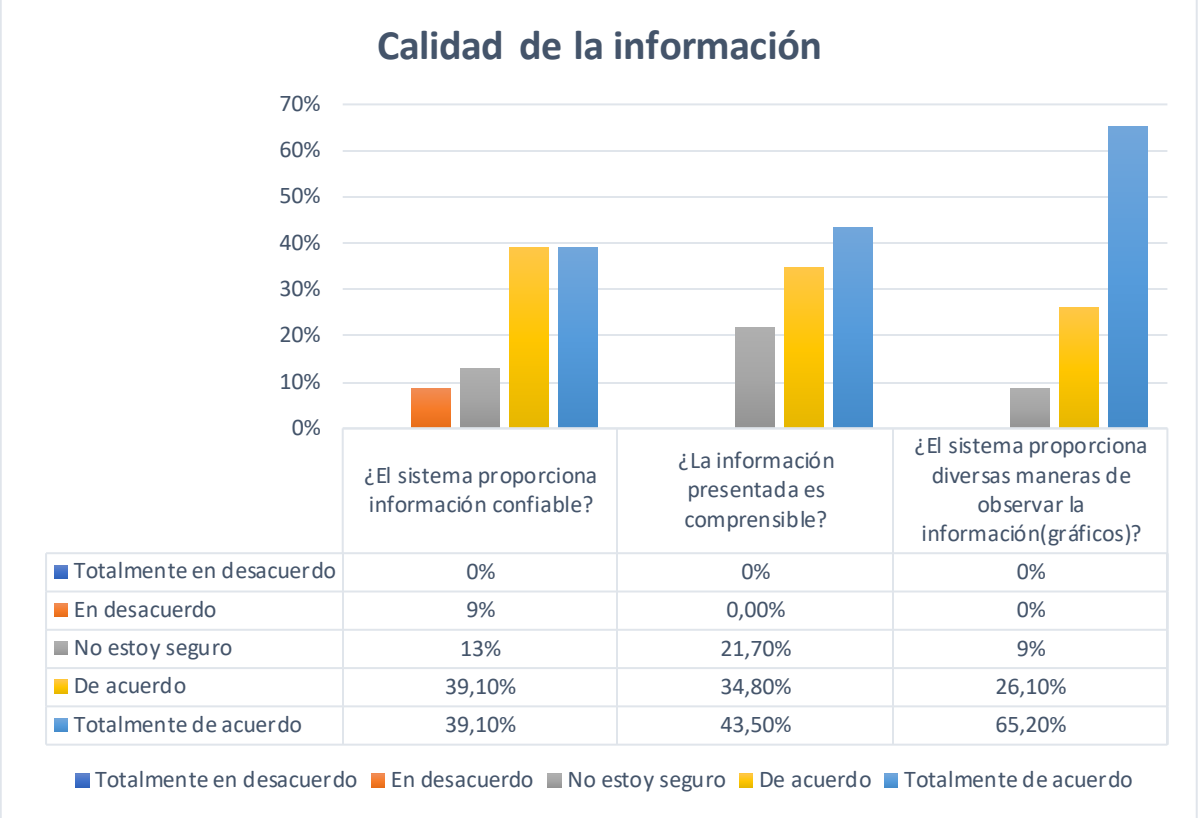
	¿Es fácil de utilizar el sistema?	¿Encuentro la interfaz muy amigable e intuitiva?	¿Es fácil de acceder?
Totalmente en desacuerdo	0%	0%	0%
En desacuerdo	0%	4,30%	0%
No estoy seguro	0%	21,70%	0%
De acuerdo	30,40%	69,60%	39,10%
Totalmente de acuerdo	69,60%	4,30%	60,90%

Figura 3.4. Calidad del sistema - Elector

En la figura 3.4 se puede apreciar resultados mayormente positivos referentes a la dimensión de la calidad del sistema. Los encuestados consideran que el sistema es fácil de usar y fácil acceder ya que el 100% está de acuerdo y totalmente de acuerdo con estas medidas. Sin embargo, el 4,3% de los encuestados no encuentran una interfaz muy amigable e intuitiva, por lo tanto, se podría mejorar este aspecto con la finalidad de obtener una mayor calidad del sistema.

Calidad de la información

La calidad de la información hace referencia al contenido que produce el sistema, el cual es de utilidad para el usuario. Los factores que se deben considerar en la calidad de la información son: consistencia, fiabilidad, confiabilidad, relevancia y comprensibilidad.



	¿El sistema proporciona información confiable?	¿La información presentada es comprensible?	¿El sistema proporciona diversas maneras de observar la información(gráficos)?
Totalmente en desacuerdo	0%	0%	0%
En desacuerdo	9%	0,00%	0%
No estoy seguro	13%	21,70%	9%
De acuerdo	39,10%	34,80%	26,10%
Totalmente de acuerdo	39,10%	43,50%	65,20%

Figura 3.5. Calidad de la información - Elector

En cuanto a la calidad de la información, en la figura 3.5 se puede apreciar que el 79,20% de los encuestado considera que la información que proporciona el sistema es confiable, debido a que están totalmente de acuerdo y de acuerdo con esta medida. Sin embargo, existe un 13% los cuales no están seguros y un 9% se encuentran en desacuerdo, ante ello se puede decir que la información presentada en el módulo del elector es netamente proporcionada por la plataforma blockchain de Polygon. Además, tanto la comprensibilidad e interpretación de la información tienden a tener una gran aceptación. Esto quiere decir que la calidad de la información es buena.

Calidad del servicio

La calidad del servicio se mide en base al soporte y asistencia por parte del desarrollador del software o del departamento de TI, considerando las capacitaciones como parte de esta categoría. Además, se debe tomar en cuenta la disponibilidad del sistema en todo momento y el cumplimiento sus funcionalidades.

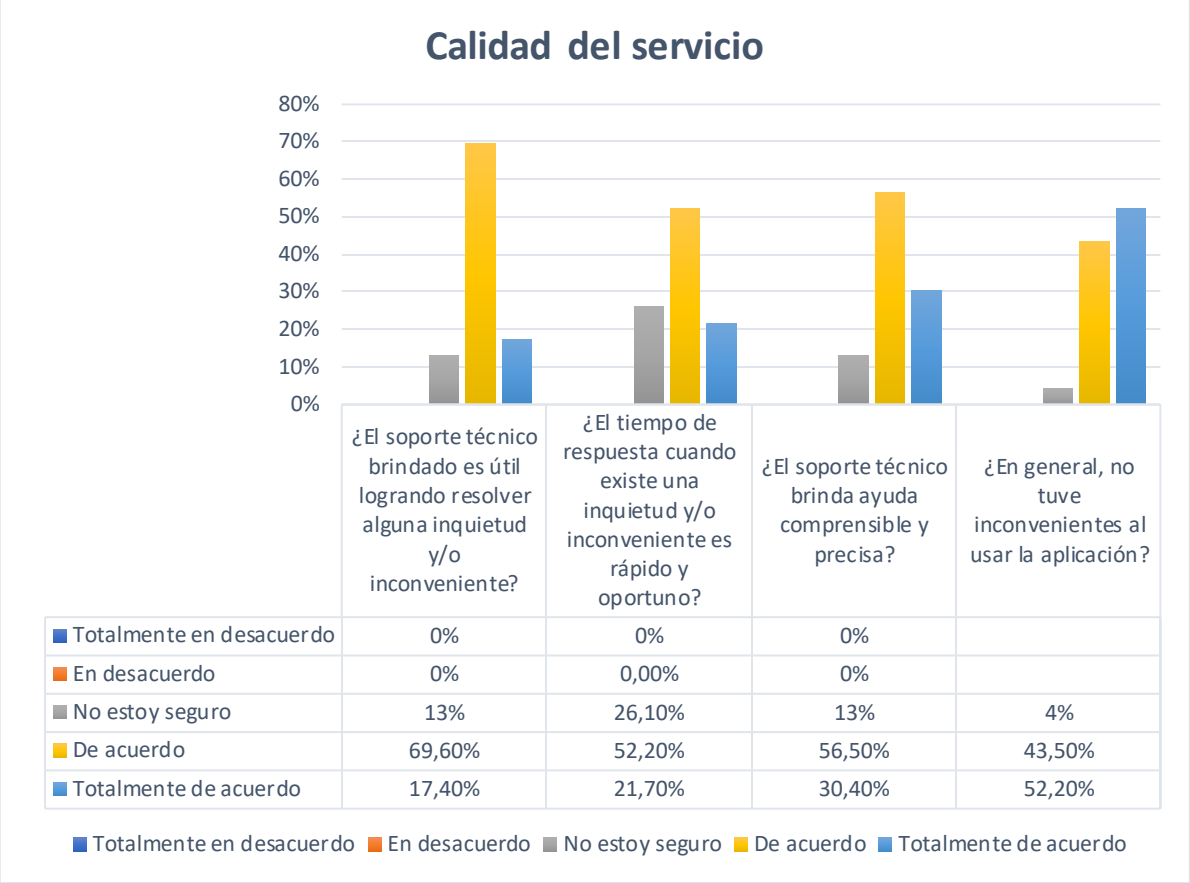
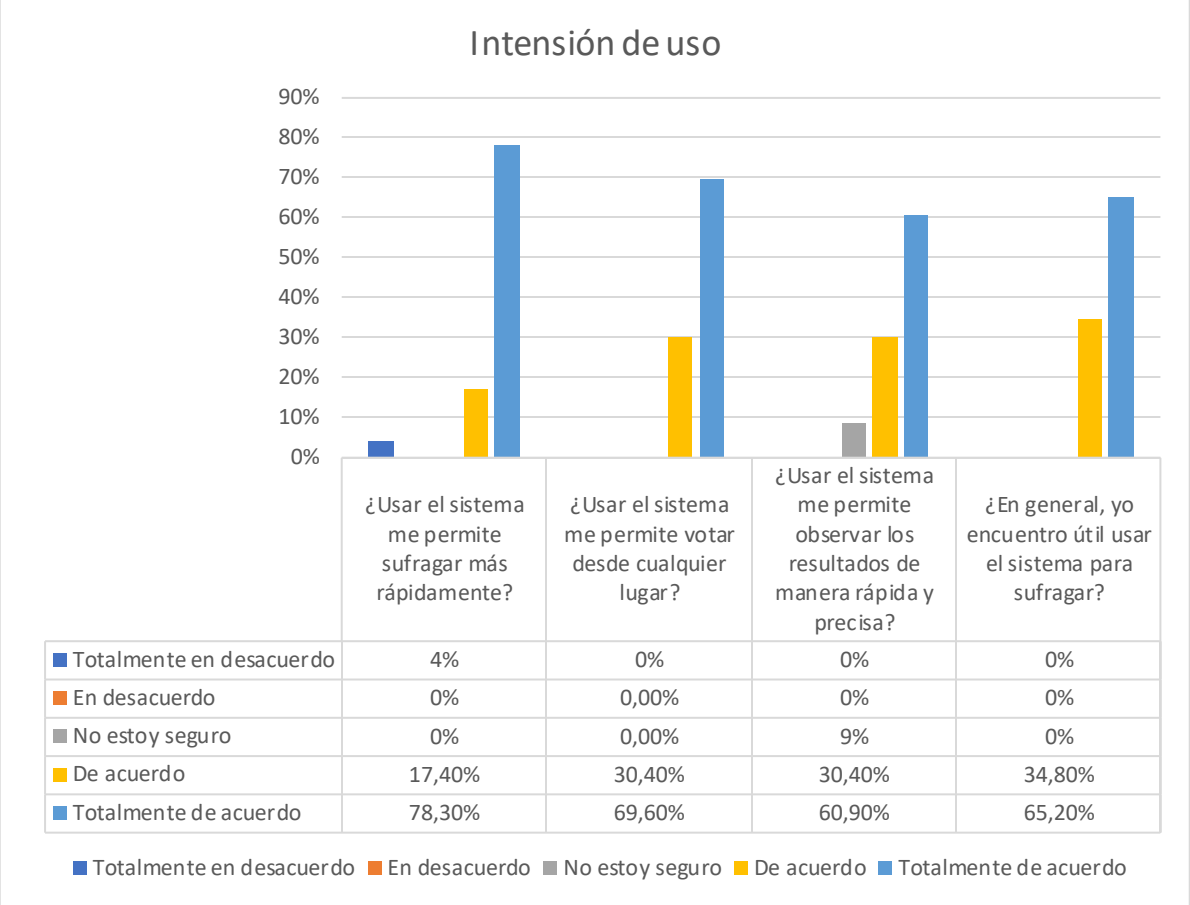


Figura 3.6. Calidad del servicio - Elector

En la figura 3.6 se puede apreciar que el 96% de los encuestados no tuvieron inconvenientes al usar la aplicación y el 4% no está seguro o tuvo algún inconveniente, por tanto, el soporte o ayuda técnica recibida por parte del desarrollador tiene un valor por encima del 70%, la cual corresponde a un soporte técnico rápido, comprensible y útil, todo esto a causa de pocos inconvenientes, consiguiendo solventarlos de manera rápida y precisa.

Intensión de uso

La intención de uso es el propósito con el que los usuarios utilizan las funcionalidades del sistema. Los factores por considerar son: frecuencia de uso, naturaleza de uso y adecuación de uso.



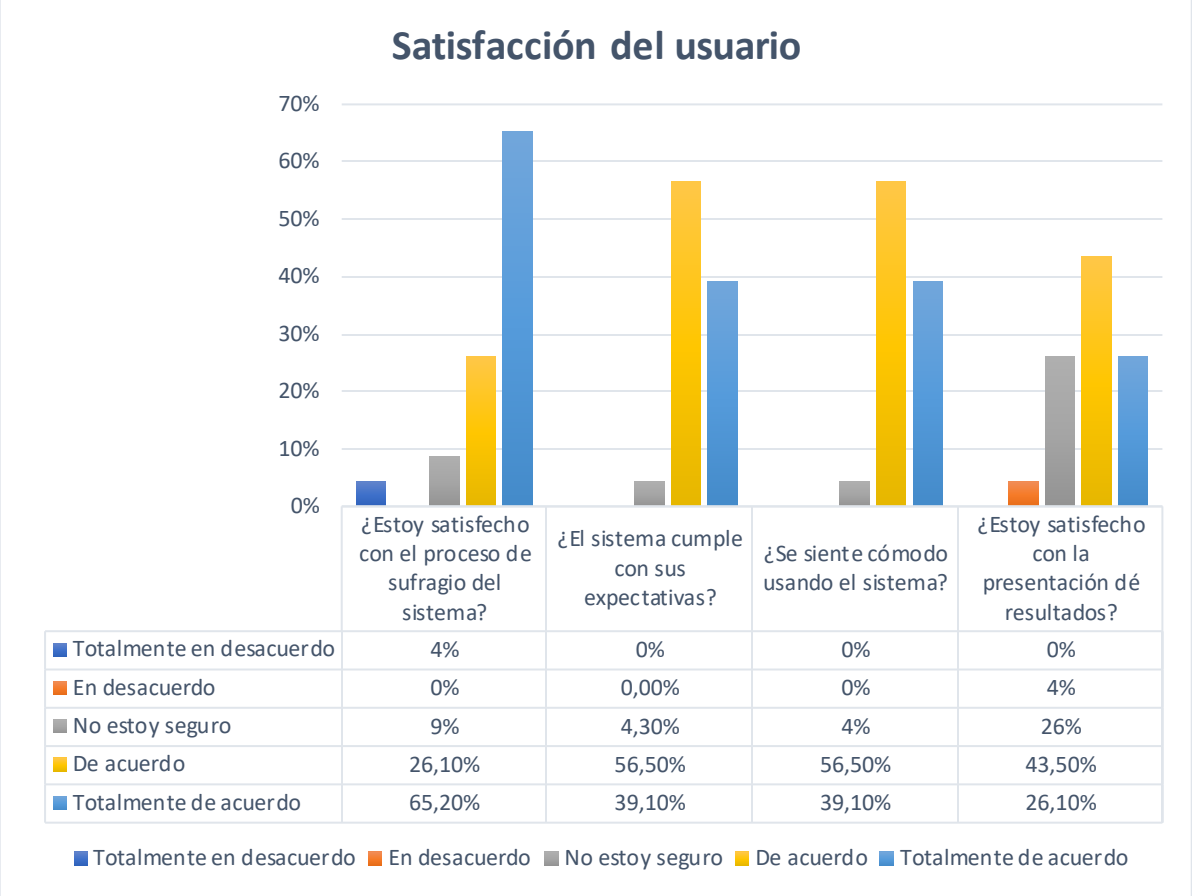
	¿Usar el sistema me permite sufragar más rápidamente?	¿Usar el sistema me permite votar desde cualquier lugar?	¿Usar el sistema me permite observar los resultados de manera rápida y precisa?	¿En general, yo encuentro útil usar el sistema para sufragar?
Totalmente en desacuerdo	4%	0%	0%	0%
En desacuerdo	0%	0,00%	0%	0%
No estoy seguro	0%	0,00%	9%	0%
De acuerdo	17,40%	30,40%	30,40%	34,80%
Totalmente de acuerdo	78,30%	69,60%	60,90%	65,20%

Figura 3.7. Intensión de uso - Elector

Como se puede apreciar en la figura 3.7 el 100% de los encuestados encuentran útil usar el sistema para sufragar. Además, más del 85% de los encuestados están de acuerdo con lo que les facilita el sistema: sufragar más rápidamente, votar desde cualquier lugar y resultados de manera rápida y precisa. Sin embargo, se puede mejorar la presentación de resultados y la velocidad de sufragio para tener una completa aceptación.

Satisfacción del usuario

Esta variable trata de identificar si el sistema cumple con las expectativas del usuario y que tan satisfecho se encuentra al momento de interactuar con el sistema, si están de acuerdo con la información presentada y si piensan seguir usando el sistema para siguientes elecciones.



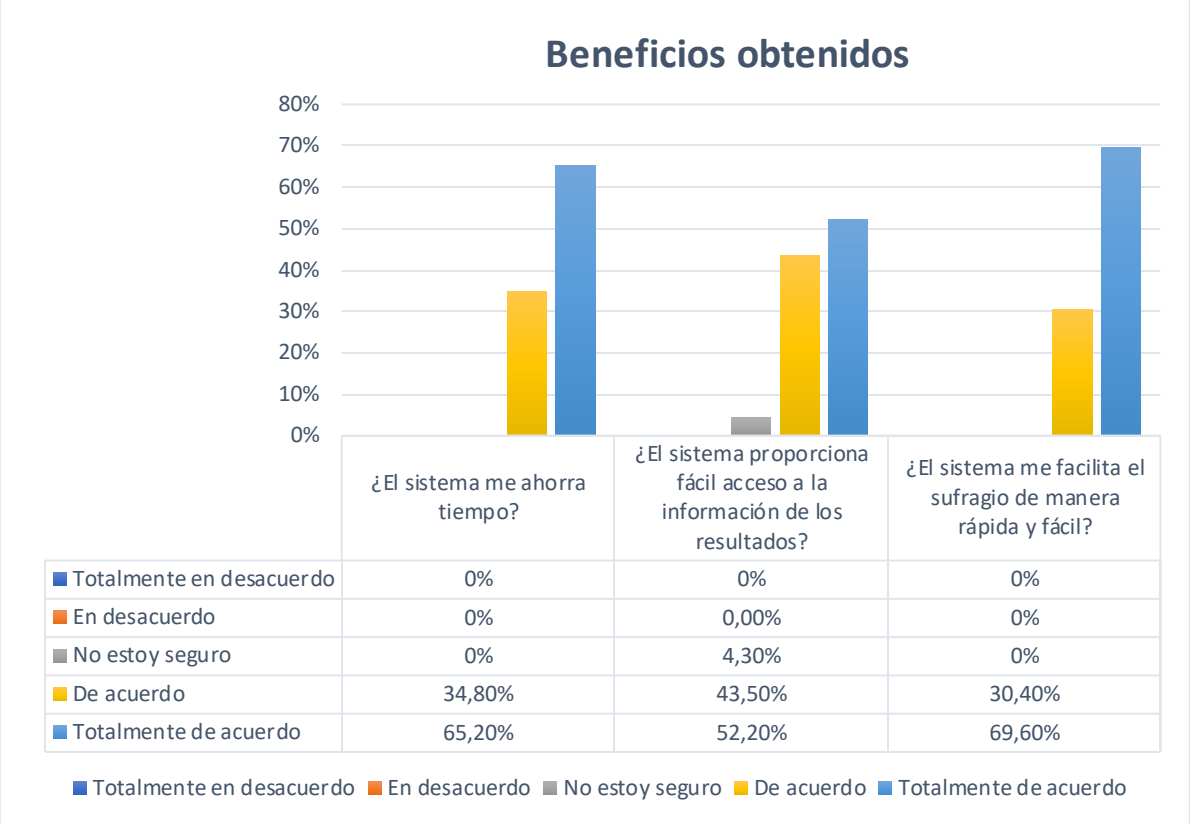
	¿Estoy satisfecho con el proceso de sufragio del sistema?	¿El sistema cumple con sus expectativas?	¿Se siente cómodo usando el sistema?	¿Estoy satisfecho con la presentación dé resultados?
Totalmente en desacuerdo	4%	0%	0%	0%
En desacuerdo	0%	0,00%	0%	4%
No estoy seguro	9%	4,30%	4%	26%
De acuerdo	26,10%	56,50%	56,50%	43,50%
Totalmente de acuerdo	65,20%	39,10%	39,10%	26,10%

Figura 3.8. Satisfacción del usuario - Elector

En la figura 3.8 se puede apreciar que el 96% de los encuestados se siente cómodo utilizando el sistema, mientras que el 4% no está muy seguro. Además, el 91% está satisfecho con el proceso de sufragio y el 95,70% de los encuestados comprueban que el sistema cumple con sus expectativas. Sin embargo, el 69,60% está satisfecho con la presentación de resultados y el 26% no está muy seguro, por tanto, es un aspecto que puede mejorarse para conseguir una completa satisfacción y por ende mejores beneficios.

Beneficios obtenidos

Esta variable se refiere a los beneficios que le atribuye al usuario al utilizar el sistema, es decir, en que le puede facilitar al usuario el uso de un sistema de votación electrónica.



	¿El sistema me ahorra tiempo?	¿El sistema proporciona fácil acceso a la información de los resultados?	¿El sistema me facilita el sufragio de manera rápida y fácil?
Totalmente en desacuerdo	0%	0%	0%
En desacuerdo	0%	0,00%	0%
No estoy seguro	0%	4,30%	0%
De acuerdo	34,80%	43,50%	30,40%
Totalmente de acuerdo	65,20%	52,20%	69,60%

Figura 3.9. Beneficios obtenidos - Elector

Finalmente, en la figura 3.9 se pueden apreciar los beneficios del sistema para el usuario final, en este caso se puede destacar que al 100% de los encuestados les permite sufragar de manera rápida y fácil, además, al 96% le ahorra tiempo y al 95,70% les facilita el acceso a los resultados de manera fácil. Por lo tanto, podemos deducir que el sistema en general aporta un gran beneficio a los electores en un proceso de votación electrónica.

3.2.3 Análisis de favorabilidad y desfavorabilidad

Se procede con el Análisis de favorabilidad y desfavorabilidad por dimensión, lo que se traduce en un análisis de apreciación para cada dimensión. Si la persona encuestada marcó “en desacuerdo” o “totalmente en desacuerdo” indica desfavorabilidad. Por otro lado, si la persona marcó “de acuerdo” o “totalmente de acuerdo” este indica favorabilidad. Si la persona no ha indicado favorabilidad o desfavorabilidad se considera indecisión.

Primero se realizó el cálculo promediando los porcentajes de las medidas correspondientes a cada dimensión, esto significa que, por defecto, se asume que todos los aspectos tienen la misma relevancia. La Tabla 3.6 muestra los porcentajes calculados.

Tabla 3.6: Resultados de favorabilidad por dimensión

Dimensión	Favorabilidad	Desfavorabilidad	Indecisión
Calidad del sistema	91.3%	1.43%	7.27%
Calidad de la información	82.6%	3%	14.4%
Calidad del servicio	85.87%	0%	14.3%
Intención de uso	96.75%	1%	2.25%
Satisfacción del usuario	88.02%	1.13%	10.85%
Beneficios netos	98.56%	0%	1.44%

Discusión de resultados

Entre lo más relevante, se puede mencionar que las dimensiones más exitosas determinadas por el estudio son los beneficios netos (98,56% de favorabilidad), la intensión de uso (96,75% de favorabilidad), calidad del sistema (91,3% de favorabilidad), calidad del servicio (85,87% de favorabilidad) y satisfacción del usuario (88,02% de favorabilidad). Es importante destacar que la dimensión de la Calidad de la información es la que tiene una menor evaluación (82,6% de favorabilidad y un 14.4% de indecisión), debido a que se ven afectados dentro de esta dimensión aspectos como la confiabilidad, comprensibilidad y presentación de la información. Sin embargo, se identifican las oportunidades de mejora en las dimensiones con menor porcentaje con la finalidad de obtener el éxito en el sistema desarrollado.

Finalmente, gracias al análisis de favorabilidad se puede apreciar que el sistema tiene una buena aceptación por parte de los usuarios con un porcentaje mínimo de favorabilidad de 82.6%, por lo tanto, se puede decir que el sistema de votación electrónica desarrollado es exitoso.

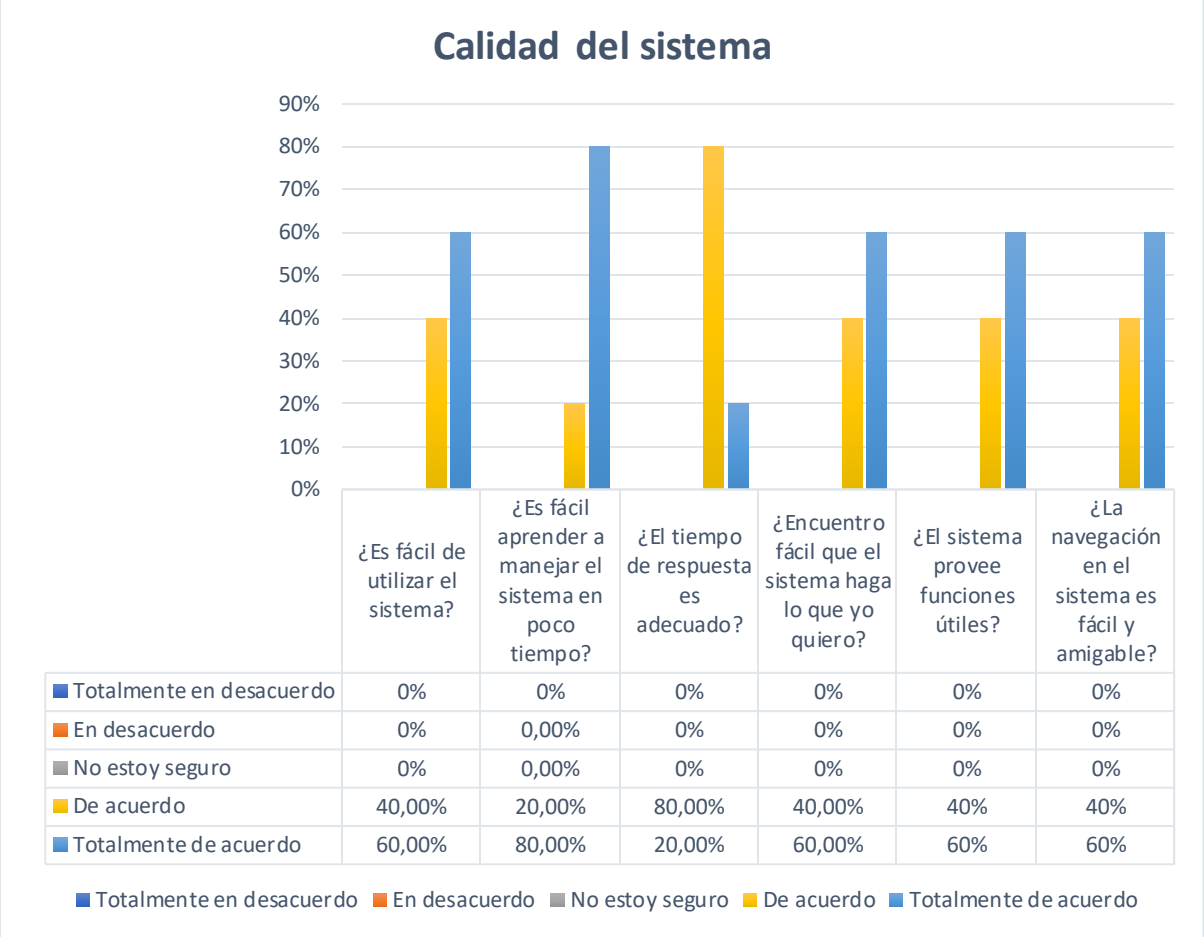
3.2.4 Variables del modelo de DeLone y McLean (Administradores)

En este apartado se presenta los resultados del cuestionario dirigido a los 5 usuarios administradores, los cuales utilizaron el sistema para la gestión de elecciones, este cuestionario se basa en las dimensiones del modelo de DeLone y McLean. Las respuestas son de escala tipo Likert con un valor de 1 a 5, donde 1 corresponde a un total desacuerdo o inconformidad y 5 corresponde a una completa aceptación por parte del usuario. A continuación, se expone los resultados obtenidos.

A diferencia del anterior análisis, este análisis se basa únicamente en los resultados obtenidos debido a la magnitud de los usuarios que utilizaron el sistema, por lo cual los resultados no varían en gran medida.

Calidad del sistema

La calidad del sistema es una característica que incluye medidas normalmente centradas en aspectos de usabilidad y rendimiento del sistema, por lo tanto, se debe tomó en cuenta las siguientes medidas: facilidad de uso, facilidad de aprendizaje, tiempo de respuesta, flexibilidad y la interactividad con el usuario.



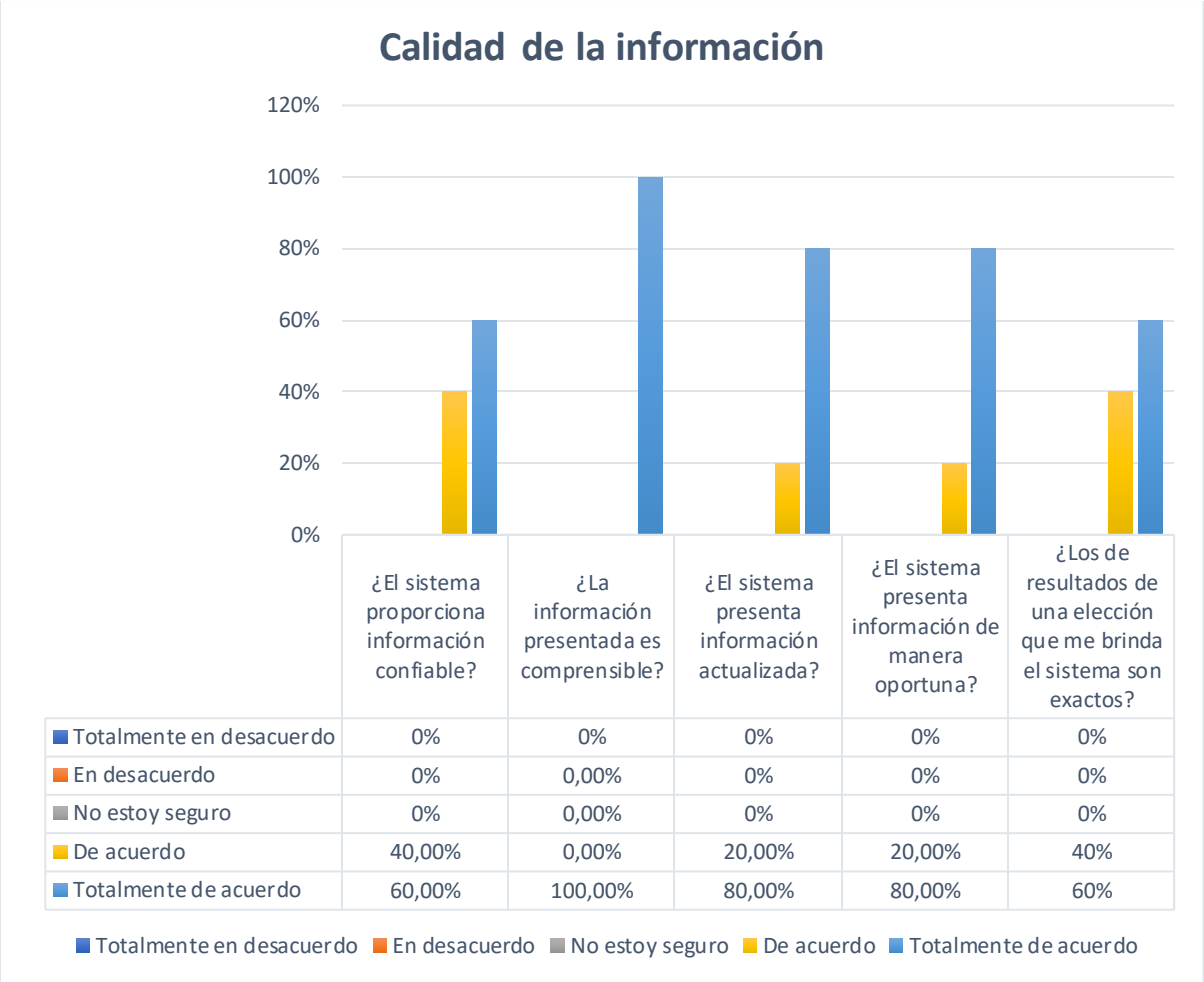
	¿Es fácil de utilizar el sistema?	¿Es fácil aprender a manejar el sistema en poco tiempo?	¿El tiempo de respuesta es adecuado?	¿Encuentro fácil que el sistema haga lo que yo quiero?	¿El sistema provee funciones útiles?	¿La navegación en el sistema es fácil y amigable?
Totalmente en desacuerdo	0%	0%	0%	0%	0%	0%
En desacuerdo	0%	0,00%	0%	0%	0%	0%
No estoy seguro	0%	0,00%	0%	0%	0%	0%
De acuerdo	40,00%	20,00%	80,00%	40,00%	40%	40%
Totalmente de acuerdo	60,00%	80,00%	20,00%	60,00%	60%	60%

Figura 3.10. Calidad del sistema - Administrador

En la figura 3.10 se puede observar la dimensión de calidad del sistema, donde la mayoría de encuestados brindan respuestas mayormente positivas, en este caso, el 60% de los encuestados está totalmente de acuerdo que el sistema es fácil de utilizar y el 40% está de acuerdo. Además, el 80% afirma que el sistema es fácil de aprender a manejar en poco tiempo, asimismo, el tiempo de respuesta es adecuado. En cuanto a la flexibilidad, navegación e interactividad, la mayoría de encuestados brinda respuestas positivas, por lo tanto, se considera que el sistema tiene una buena calidad.

Calidad de la información

La calidad de la información hace referencia al contenido que produce el sistema, el cual es de utilidad para el usuario. Los factores que se tomaron en consideración en la calidad de la información son: consistencia, fiabilidad, confiabilidad, relevancia y comprensibilidad.



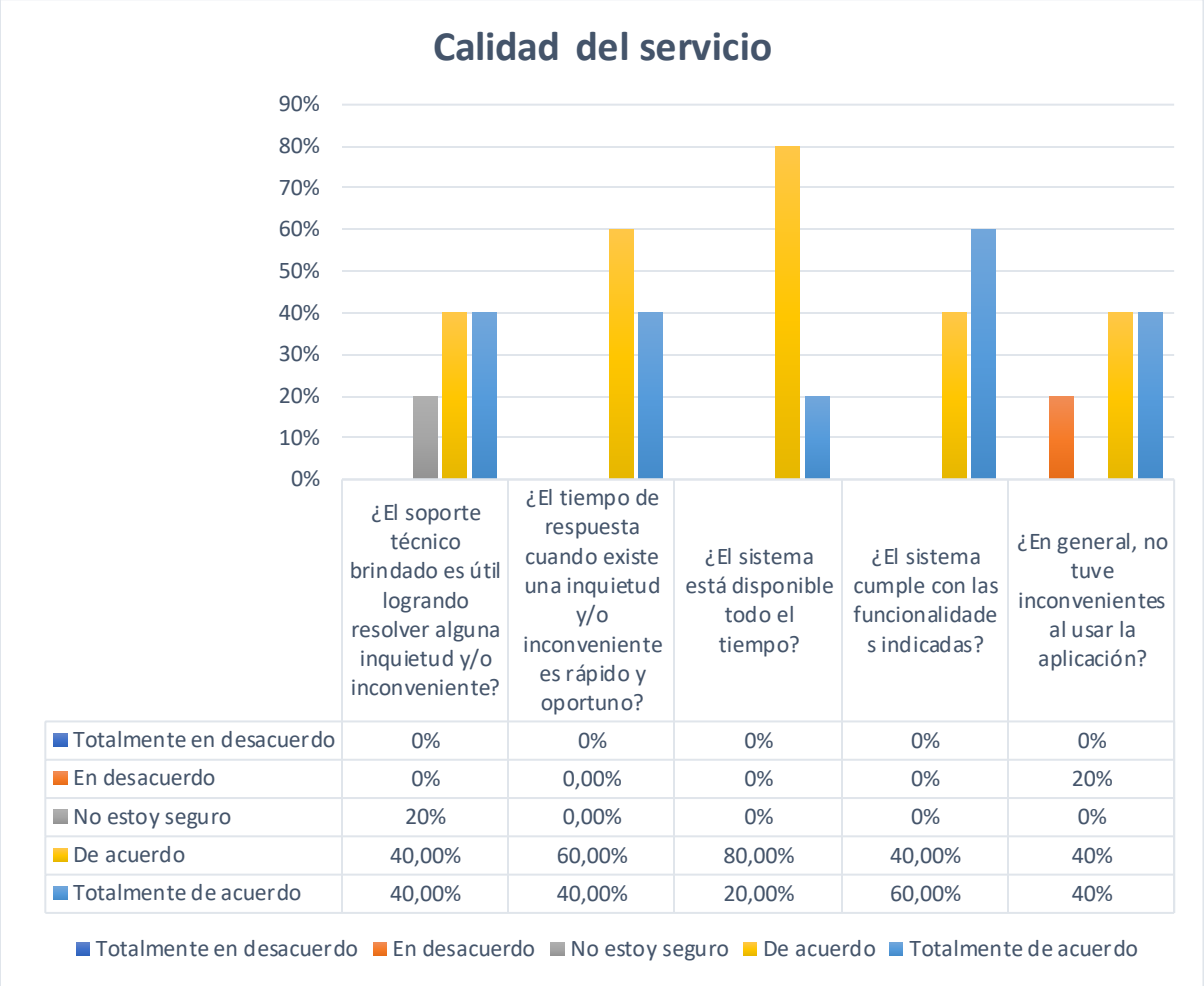
	¿El sistema proporciona información confiable?	¿La información presentada es comprensible?	¿El sistema presenta información actualizada?	¿El sistema presenta información de manera oportuna?	¿Los de resultados de una elección que me brinda el sistema son exactos?
Totalmente en desacuerdo	0%	0%	0%	0%	0%
En desacuerdo	0%	0,00%	0%	0%	0%
No estoy seguro	0%	0,00%	0%	0%	0%
De acuerdo	40,00%	0,00%	20,00%	20,00%	40%
Totalmente de acuerdo	60,00%	100,00%	80,00%	80,00%	60%

Figura 3.11. Calidad de la información - Administrador

Como se puede apreciar en la figura 3.11 tenemos resultados mayormente positivos en la dimensión de calidad de la información, por lo cual, se puede decir que tenemos una buena calidad en nuestro sistema de votación. Los encuestados están en total acuerdo y de acuerdo respectivamente con las siguientes afirmaciones: la confiabilidad del sistema, presentación de información comprensible y la precisión de los resultados en una elección, teniendo un 80% de aceptación total por parte de los usuarios.

Calidad del servicio

La calidad del servicio se mide en base al soporte y asistencia por parte del desarrollador del software o del departamento de TI, considerando las capacitaciones como parte de esta categoría. Además, se tomaron en consideración la disponibilidad del sistema en todo momento, solución de inconvenientes presentado y el cumplimiento sus funcionalidades.



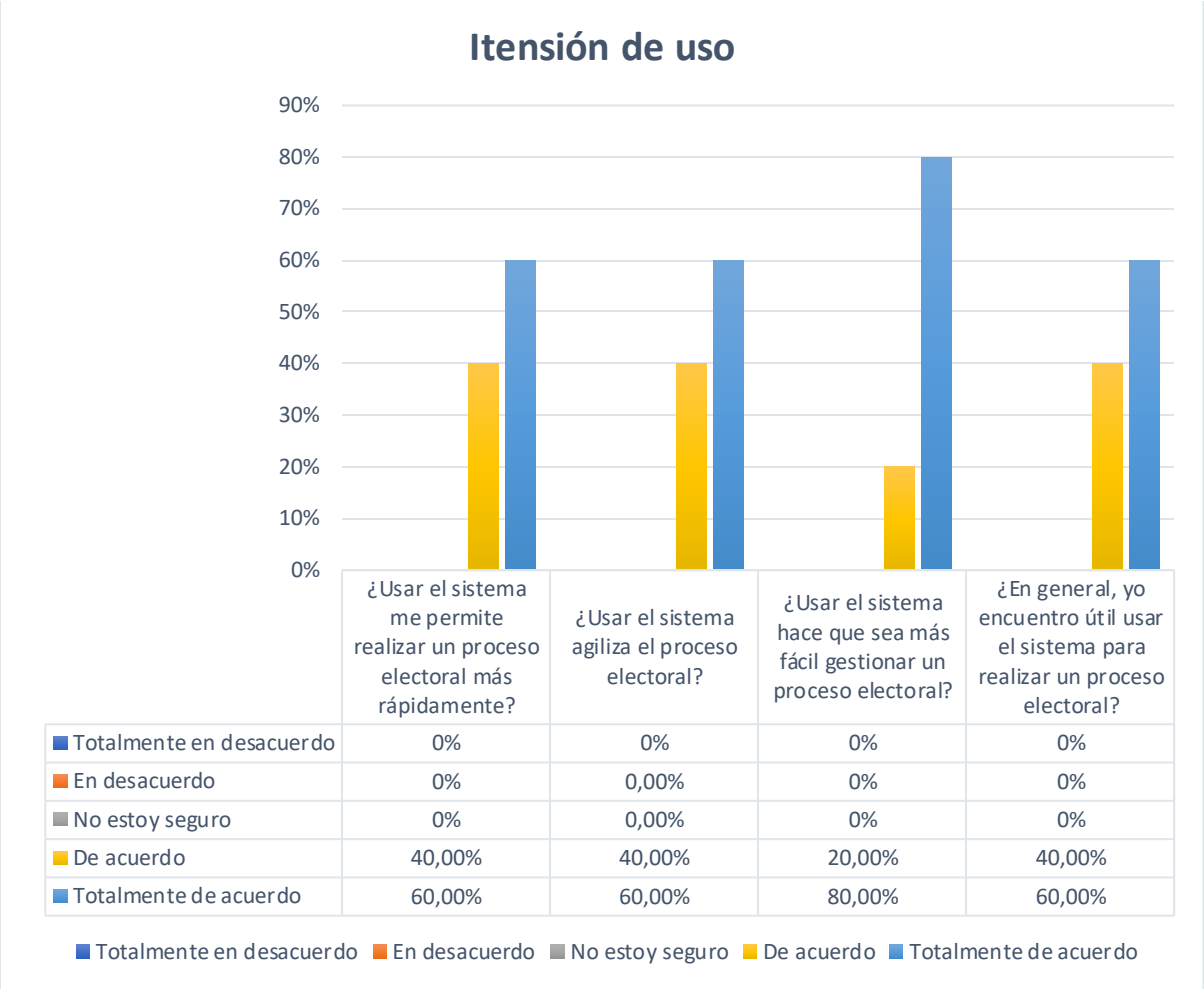
	¿El soporte técnico brindado es útil logrando resolver alguna inquietud y/o inconveniente?	¿El tiempo de respuesta cuando existe una inquietud y/o inconveniente es rápido y oportuno?	¿El sistema está disponible todo el tiempo?	¿El sistema cumple con las funcionalidades indicadas?	¿En general, no tuve inconvenientes al usar la aplicación?
Totalmente en desacuerdo	0%	0%	0%	0%	0%
En desacuerdo	0%	0,00%	0%	0%	20%
No estoy seguro	20%	0,00%	0%	0%	0%
De acuerdo	40,00%	60,00%	80,00%	40,00%	40%
Totalmente de acuerdo	40,00%	40,00%	20,00%	60,00%	40%

Figura 3.12 Calidad del servicio - Administrador

En la figura 3.12 se presentan los resultados mayormente positivos de la calidad del servicio, estos resultados se basan principalmente en la ayuda recibida por parte del desarrollador en caso de existir inconvenientes al momento de realizar una gestión de elecciones, en este caso podemos observar que el 80% de los encuestados no tuvo algún inconveniente al momento de utilizar el sistema pero el 20%, si lo tuvo, por lo tanto, la ayuda brindada a dichos usuarios ha sido calificada como buena a excelente debido a una baja cantidad de usuarios que necesitaron soporte o ayuda técnica. Finalmente, se puede deducir que el soporte brindado es bueno con una aceptación de 80-100%.

Intensión de uso

La intención de uso es el propósito con el que los usuarios utilizan las funcionalidades del sistema. Los factores por considerar son: frecuencia de uso, naturaleza de uso y adecuación de uso.



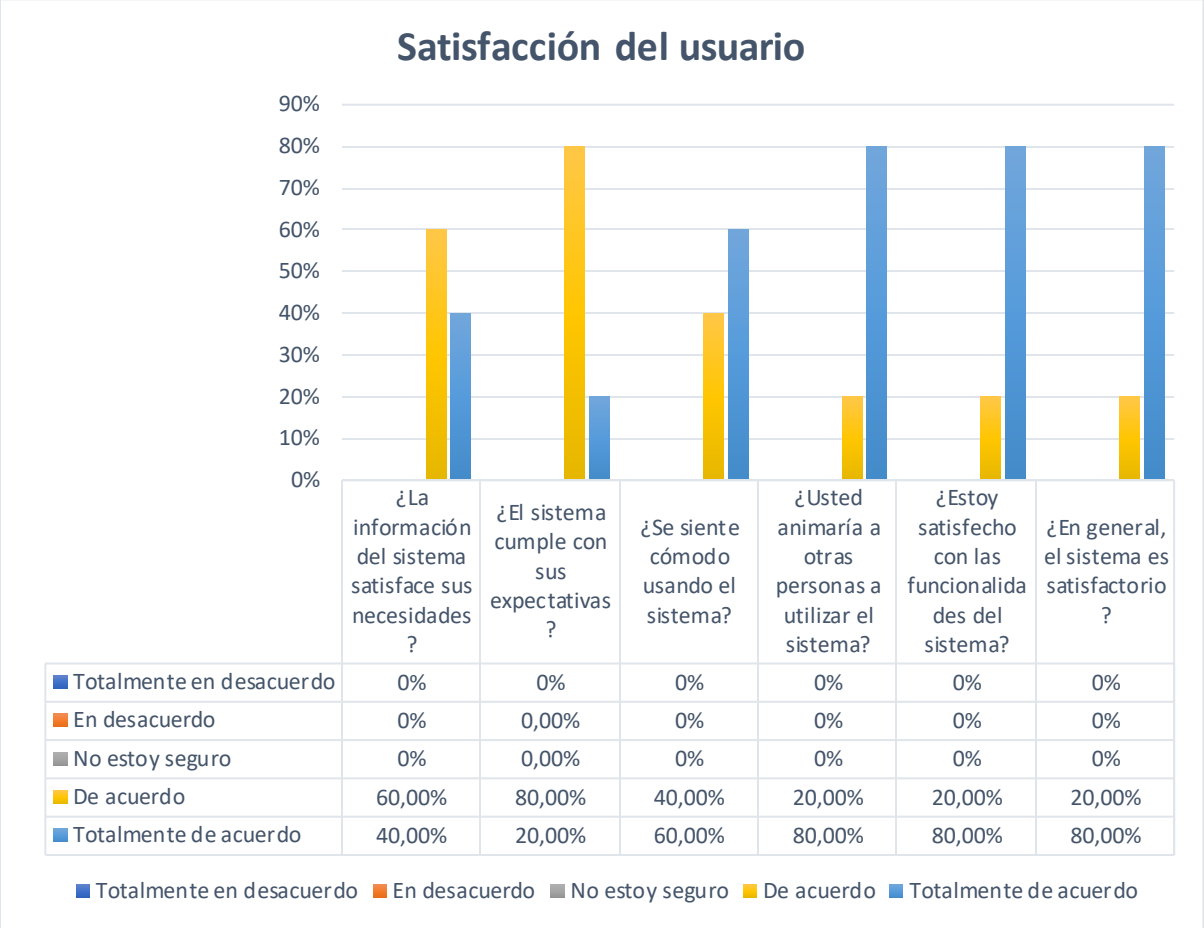
	¿Usar el sistema me permite realizar un proceso electoral más rápidamente?	¿Usar el sistema agiliza el proceso electoral?	¿Usar el sistema hace que sea más fácil gestionar un proceso electoral?	¿En general, yo encuentro útil usar el sistema para realizar un proceso electoral?
Totalmente en desacuerdo	0%	0%	0%	0%
En desacuerdo	0%	0,00%	0%	0%
No estoy seguro	0%	0,00%	0%	0%
De acuerdo	40,00%	40,00%	20,00%	40,00%
Totalmente de acuerdo	60,00%	60,00%	80,00%	60,00%

Figura 3.13 Intensión de uso - Administrador

Los resultados obtenidos para este aparado son realmente positivos, el 60% de los encuestados están totalmente de acuerdo que el sistema les permite realizar un proceso electoral más rápidamente y el 40% restante está de acuerdo. Además, afirman que el sistema agiliza el proceso electoral, facilita la gestión y lo encuentran útil para realizar un proceso electoral, estas afirmaciones están basadas en sus respuestas, tal y como se puede apreciar en la figura 3.13, obteniendo así, una completa aceptación por parte de los usuarios administradores.

Satisfacción del usuario

Esta variable trata de identificar si el sistema cumple con las expectativas del usuario y que tan satisfecho se encuentra al momento de interactuar con el sistema, si están de acuerdo con la información presentada y si piensan seguir usando el sistema para siguientes elecciones.



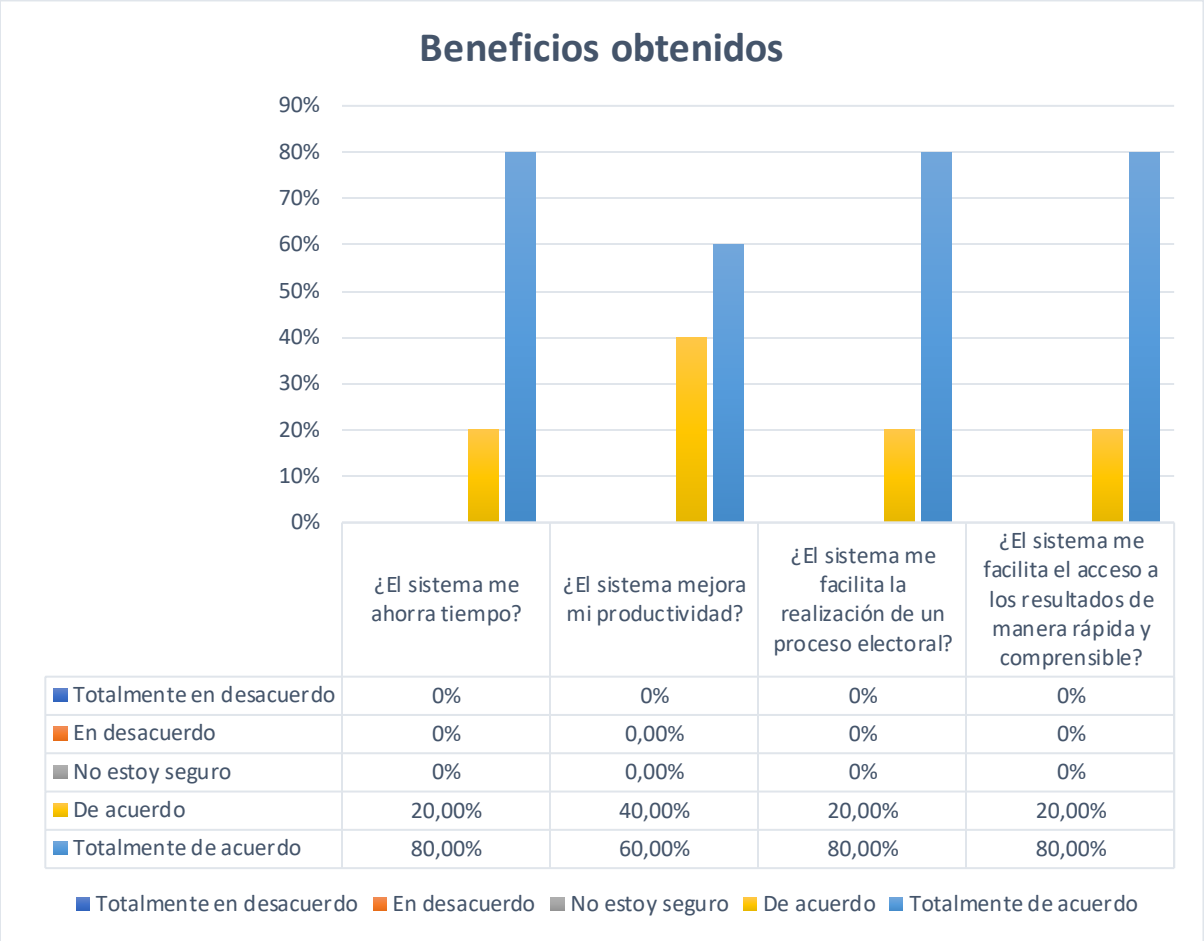
	¿La información del sistema satisface sus necesidades ?	¿El sistema cumple con sus expectativas ?	¿Se siente cómodo usando el sistema?	¿Usted animaría a otras personas a utilizar el sistema?	¿Estoy satisfecho con las funcionalidades del sistema?	¿En general, el sistema es satisfactorio ?
Totalmente en desacuerdo	0%	0%	0%	0%	0%	0%
En desacuerdo	0%	0,00%	0%	0%	0%	0%
No estoy seguro	0%	0,00%	0%	0%	0%	0%
De acuerdo	60,00%	80,00%	40,00%	20,00%	20,00%	20,00%
Totalmente de acuerdo	40,00%	20,00%	60,00%	80,00%	80,00%	80,00%

Figura 3.14. Satisfacción del usuario – Administrador

Como se puede apreciar en la figura 3.14 el 40% de los encuestados están totalmente de acuerdo con la información del sistema por lo cual satisface sus necesidades, mientras que el 60% está de acuerdo con esta medida. Además, para el 80% de los encuestados están de acuerdo que el sistema cumple con sus expectativas y el 20% están totalmente de acuerdo. Cabe mencionar que la comodidad que brinda el sistema, las funcionalidades y la satisfacción general del uso del sistema, tienen una completa aceptación por parte de los encuestados, a causa de ello, los encuestados podrían animar a otros usuarios a utilizar el sistema desarrollado.

Beneficios obtenidos

Esta variable se refiere a los beneficios que le atribuye al usuario al utilizar el sistema, es decir, en que le puede facilitar al usuario el uso de un sistema de votación electrónica.



	¿El sistema me ahorra tiempo?	¿El sistema mejora mi productividad?	¿El sistema me facilita la realización de un proceso electoral?	¿El sistema me facilita el acceso a los resultados de manera rápida y comprensible?
Totalmente en desacuerdo	0%	0%	0%	0%
En desacuerdo	0%	0,00%	0%	0%
No estoy seguro	0%	0,00%	0%	0%
De acuerdo	20,00%	40,00%	20,00%	20,00%
Totalmente de acuerdo	80,00%	60,00%	80,00%	80,00%

Figura 3.15. Beneficios obtenidos - Administrador

Finalmente, tenemos los beneficios que obtienen los usuarios al utilizar el sistema, esto como resultado de la intensión de uso y la satisfacción del usuario ya que, si no tuviera una buena satisfacción no se podrían conseguir beneficios que aporten al usuario y de la misma manera con la intensión de uso. En la figura 3.15 se puede observar que al 80% de los encuestados les ahorra tiempo el uso del sistema, estando totalmente de acuerdo con la afirmación y el 20% restante está de acuerdo. Además, mejora su productividad, permitiéndoles realizar diferentes tareas mientras usan el sistema, sin mencionar que, al usar el sistema les facilita la realización de un proceso electoral, así como también sus resultados de manera rápida y comprensible.

CONCLUSIONES

- Actualmente, existen diversos sistemas de voto electrónico, sin embargo, a causa de la inserción de la tecnología dentro de un proceso electoral, también han surgido vulnerabilidades y ataques a estos sistemas informáticos, lo cual disminuye la confianza y participación en estos sistemas. Para afrontar dichas deficiencias, se utiliza la tecnología blockchain para mejorar los niveles de confiabilidad en el almacenamiento de votos, escrutinio y emisión de resultados.

- Tras la revisión de literatura, podemos deducir que el uso de la tecnología blockchain en un proceso electoral presenta los siguientes beneficios: disponibilidad, integridad, trazabilidad, privacidad e inmutabilidad. Sin duda, provee soluciones a los sistemas de votación electrónica tradicionales, con el objetivo de evitar fraudes y generar una mayor confianza en los electores.

- Como se ha podido observar, se desarrolló el sistema usando la metodología Scrum, la cual proporcionó una mejora continua del sistema a través de sus iteraciones, cumpliendo así, con éxito los requerimientos planteados en el tiempo especificado. En este contexto, se inició con la definición de roles, las historias de usuario, y posteriormente se planificó los Sprints con sus respectivas tareas hasta finalizar con el desarrollo.

- El sistema desarrollado permite la creación de un proceso electoral y gracias a la implementación de un contrato inteligente en la red blockchain, obtiene las funcionalidades para el sufragio, escrutinio y emisión de resultados de manera descentralizada e inmutable. Además, provee resultados transparentes y accesibles debido a su implementación en una blockchain pública.

- El sistema que se desarrolló permite el inicio de sesión mediante el rol administrador y elector, el administrador puede realizar la gestión de elecciones, listas, candidatos y usuarios, además, permite agregar las listas a la blockchain para posteriormente realizar el proceso de sufragio y escrutinio con ayuda de la tecnología blockchain.

- Para medir el éxito y eficacia del sistema desarrollado se realizó la validación mediante el modelo de éxito de DeLone y McLean, considerando las categorías de: calidad del sistema, calidad de la información, calidad de servicio, intensión de uso, satisfacción

del usuario y sus impactos netos, obteniendo una buena aceptación por parte de los usuarios con un porcentaje mínimo de favorabilidad de 82.6%, por lo tanto, se puede decir que el sistema de votación electrónica desarrollado es exitoso.

- Polygon es una plataforma de escalado para Ethereum, si bien es cierto, existen varias soluciones de escalado, Polygon nos ofrece transacciones más rápidas y tarifas relativamente bajas, debido a que la plataforma cuenta con su propia moneda, MATIC, y su precio fluctúa entre 1.50 USD mientras que un ETH fluctúa entre 3.000 USD. Además, un aspecto importante a considerar es su seguridad, la cual tiende a beneficiarse de los nodos validadores de Ethereum.

RECOMENDACIONES

- Para obtener resultados relevantes mediante la revisión de literatura, en primer lugar, se debe considerar que es lo que se quiere buscar, definiendo la unidad de análisis y preguntas de investigación. Luego, generar una cadena de búsqueda que nos ayude a filtrar los artículos que respondan las preguntas de investigación, cabe desacatar que la información debe ser recolectada de fuentes bibliográficas reconocidas, con el fin de obtener información que aporte a la investigación.

- Con el fin de obtener un producto de software con mayor calidad, es recomendable utilizar una metodología que nos facilite el proceso de desarrollo, en este caso se utilizó Scrum, la cual mediante iteraciones permite una mejora continua al producto. Sin embargo, para utilizar una metodología, es fundamental investigar y leer la documentación, para así obtener el conjunto de buenas prácticas que nos ofrece.

- Para crear aplicaciones que usen la tecnología blockchain (DApps), es recomendable conocer el funcionamiento y características de esta tecnología, esto con el fin de aprovechar al máximo sus beneficios. Además, es importante conocer algún lenguaje de programación que permita crear contratos inteligentes como lo es Solidity e investigar las diversas plataformas que existen en el ecosistema blockchain.

- Para el desarrollo de aplicaciones descentralizadas (DApps), es recomendable enviar los datos más sensibles e indispensables a la blockchain con la finalidad de no generar gastos innecesarios a largo plazo.

- Para validar la eficacia y éxito de un sistema de información, es recomendable usar el modelo de éxito de DeLone and McLean, debido a que su resultado se basa en la experiencia del usuario al utilizar el sistema desarrollado.

LIMITACIONES Y TRABAJOS FUTUROS

Debido al tiempo limitado para el desarrollo del proyecto y su alcance, se presentaron algunas limitaciones en el prototipo propuesto.

- El sistema de votación desarrollado está limitado a crear solo una elección, esto se debe a que el contrato inteligente es utilizado únicamente para el sufragio, escrutinio y emisión de resultados, por lo tanto, si se requiere realizar otra elección, se debe desplegar un nuevo contrato por cada elección en la ***blockchain*** o en su defecto desarrollar toda la lógica del sistema en el contrato inteligente, sin embargo, esto implicaría un costo por cada operación dentro del sistema.

Además, se proponen los siguientes trabajos futuros que podrán extender las funcionalidades del sistema de voto electrónico desarrollado en el presente trabajo de grado. Además, se presentan otros trabajos futuros en referencia a *blockchain*.

- Implementar un módulo de capacitación y tutoriales de emisión de votos, considerada una característica de carácter obligatorio para los de sistemas de votación electrónica.

- Implementar sistemas biométricos para verificar la identidad del votante.

- Investigar de manera más exhaustiva las soluciones de escalado de capa 2 con el objetivo de elegir la plataforma que nos atribuya menores costos en las transacciones y mayor velocidad, sin perder la seguridad y descentralización, no solo en la red de Ethereum sino también en otras redes como Bitcoin, e incluso investigar a profundidad proyectos de capa 1, todo esto debido al gran auge de plataformas y algoritmos de consenso que tiene cada una.

- Investigar las aplicaciones que tienen los contratos inteligentes en el ecosistema *blockchain**,*** por ejemplo: en seguridad automatizada, alquiler de propiedades, contratos automáticos con IoT, licencias de música, mercado de electricidad, cadenas de suministros, sectores seguros: salud, automóvil, entre otros.

REFERENCIAS

Abuidris, Y. (2021). Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *ETRI Journal*, 357-370. doi:10.4218 / etrij.2019-0362

Adebowale, O. (2017). Validation of the DeLone and McLean Information Systems Success Model. *Healthcare Informatics Research*, 60-66. doi:https://doi.org/10.4258/hir.2017.23.1.60

Agate, V., De Paola, A., Ferraro, P., Lo Re, G., & Morana, M. (2021). SecureBallot: A secure open source e-Voting system. *Journal of Network and Computer Applications*, *191*, 103165. https://doi.org/10.1016/J.JNCA.2021.103165

Agora. (s.f.). Bringing our voting systems. Obtenido de https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5f37eed8cedac41642edb534/1597501378925/Agora_Whitepaper.pdf

Amritraj, S., Kelly, C., Reza, P., Qi, Z., Ali, D., Kim, K., & Raymond, C. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications, 149*. doi:10.1016/J.JNCA.2019.102471

Aruna, Maheswari, & Saranya. (2021). Highly Secured Blockchain Based Electronic Voting System Using SHA3 and Merkle Root. doi:10.1088/1757-899X/993/1/012103

Basilius, C., Moeljono, W., & Arya, W. (2021). Go-Ethereum for electronic voting systemusing clique as proof-of-authority. *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, 1565 - 1572. doi:10.12928/TELKOMNIKA.v19i5.20415

Bernhard, P., Markus, Z., Mihai, N., & Wolfgang, S. (2010). Estimation, Constraint-Based Recommendation for Software Project Effort. *JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE*. doi:10.4304/jetwi.2.4.282-290

Binance. (2021). *Binance Smart Chain vs. Ethereum: ¿Cuál es la diferencia?* Obtenido de Binance Academy: https://academy.binance.com/es/articles/binance-smart-chain-vs-ethereum-what-s-the-difference

Coinbase. (s.f.). What is Ethereum? Obtenido de https://www.coinbase.com/es/learn/crypto-basics/what-is-ethereum#is-ethereum-secure

Coinbase. (s.f.). What is Polygon (MATIC)? Obtenido de https://www.coinbase.com/es/learn/crypto-basics/what-is-polygon

DeLone, W. H., & McLean, E. R. (2016). Information Systems Success Measurement. *Foundations and Trends® in Information Systems*, *2*(1), 1–116. https://doi.org/10.1561/2900000005

Di Francesco Maesa, D., & Mori, P. (2020). Blockchain 3.0 applications survey. *Journal of Parallel and Distributed Computing*, *138*, 99–114. https://doi.org/10.1016/J.JPDC.2019.12.019

Dhulavvagol, P. M. (2020). Blockchain Ethereum Clients Performance Analysis Considering E-Voting Application. *Procedia Computer Science, 167*, 2506-2515. doi:https://doi.org/10.1016/j.procs.2020.03.303

Duarte, M. (06 de 08 de 2018). AMERICA LATINA EN MOVIMIENTO. *Blockchain CGT* . Obtenido de https://www.alainet.org/es/articulo/194550

Friedman, N., & Ormiston, J. (2022). Blockchain as a sustainability-oriented innovation?: Opportunities for and resistance to Blockchain technology as a driver of sustainability in global food supply chains. *Technological Forecasting and Social Change*, *175*, 121403. https://doi.org/10.1016/J.TECHFORE.2021.121403

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, *177*, 102857. https://doi.org/10.1016/J.JNCA.2020.102857

Jane, W., & Richard, W. (2002). Analyzing the past to prepare for the future: writing a literature review. *MIS Quarterly*. doi:10.1016/j.freeradbiomed.2005.02.032

K, G. S., & Sree, S. T. (2021). A Secure Digital E-Voting Using Blockchain Technology. *Journal of Physics: Conference Series*, 12197. https://doi.org/10.1088/1742-6596/1916/1/012197

Kashif, K., Junaid, A., & Muhammad, K. (2020). Investigating performance constraints for blockchain based secure e-voting system. *Future Generation Computer Systems*, 13-26. doi:10.1016/J.FUTURE.2019.11.005

Khan, K. M., Arshad, J., & Khan, M. M. (2020). Investigating performance constraints for blockchain based secure e-voting system. *Future Generation Computer Systems*, *105*, 13–26. https://doi.org/10.1016/J.FUTURE.2019.11.005

Nasir, M. H., Arshad, J., Khan, M. M., Fatima, M., Salah, K., & Jayaraman, R. (2022). Scalable blockchains — A systematic review. *Future Generation Computer Systems*, *126*, 136–162. https://doi.org/10.1016/J.FUTURE.2021.07.035

Olawande, D., & Darren, T. (2020). Architecture-Centric Evaluation of Blockchain-BasedSmart Contract E-Voting for National Elections. *Informatics*. doi:10.3390 / informática7020016

Oviedo, H., & Campo-Arias, A. (2005). Aproximación al uso del coeficiente alfa. *Revista Colombiana de Psiquiatría, XXXIV*. Obtenido de http://www.scielo.org.co/pdf/rcp/v34n4/v34n4a09.pdf

Park, H.-D. (2019). A Decentralized E-Voting System Based on Blockchain Network. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 3650 - 3652. doi:10.35940/ijitee.L3815.1081219

Pawlak, M., & Poniszewska-Marańda, A. (2021). Trends in blockchain-based electronic voting systems. *Information Processing & Management*, *58*(4), 102595.

https://doi.org/10.1016/J.IPM.2021.102595

Polys. (s.f.). *Polys*. Recuperado el 06 de 01 de 2022, de https://polys.me/

S, A., M, M., & A, S. (2020). Highly Secured Blockchain Based ElectronicVoting System Using SHA3 and Merkle Root. *Materials Science and Engineering*. doi:10.1088/1757-899X/993/1/012103

Shahzad, B., & Crowcroft, J. (2019). Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access*, 24477- 24488. doi:10.1109/ACCESS.2019.2895670

Uzma, J., Mohd, J., & Zarina, S. (2021). Blockchain for Electronic Voting System—Review and OpenResearch Challenges. *Sensors*. doi:10.3390/s21175874

Voatz. (s.f.). Obtenido de https://voatz.com/security-and-technology/

Yang, X., Yi, X., Nepal, S., Kelarev, A., & Han, F. (2020). Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities. *Future Generation Computer Systems*, *112*, 859–874. https://doi.org/10.1016/J.FUTURE.2020.06.051

Yin, R. (2014). Case Study Research Design and Methods (5th ed.). Thousand Oaks. 282. doi:10.3138/cjpe.30.1.108

Yousif, A., Rajesh, K., Ting, Y., & Joseph, O. (2021). Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *Journal*, 357 - 370. doi:10.4218/etrij.2019-0362

Zhang, S., Wang, L., & Xiong, · Hu. (2020). Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security*, *19*, 323–341. https://doi.org/10.1007/s10207-019-00465-8

ANEXOS

Funciones del Smart Contract

En este apartado se explicará de manera más detallada, las funciones de nuestro contrato inteligente utilizado para nuestro sistema de votación, el cual fue desplegado en la red de pruebas de Polygon.

Como se puede apreciar en la figura 4.1, se crea un objeto para el elector y otro para la lista, con los atributos más necesarios debido a que el contrato es utilizado para el sufragio y escrutinio del sistema de votación. Además, se declara un mapping (unión de un id con un valor) de los electores y listas para vincular sus datos. Cabe destacar que, el constructor asigna como propietario del contrato a la dirección que lo desplegó en una red blockchain, mediante la cual se pueden restringir la ejecución de sus funciones.

```
contract Vote {

    struct Voter {
        uint ci;    // value unique
        bool voted; // vote unique
    }

    struct List {
        string name;   // name list
        uint voteCount; // number of accumulated votes
    }

    mapping(uint => Voter) public voters;

    constructor(){
        owner = msg.sender;
    }

    List[] public AddLists(listNames);;
```

Figura 4.1. Variables declaradas en el contrato inteligente Vote

El contrato inteligente Vote tiene las siguientes funciones:

- La función ***addLists*** se encarga de agregar las listas de una elección determinada. Recibe como parámetro un arreglo de strings con todas las listas y agrega valores a las variables de nombre y el número de votos de cada lista, en su defecto inicialmente con 0 tal y como se aprecia en la figura 4.2.

```
function AddLists(string[] memory listNames) public {
    for (uint i = 0; i < listNames.length; i++) {
        lists.push(
            List({
                name: listNames[i],
                voteCount: 0
            })
        );
    }
}
```

Figura 4.2. Contrato inteligente, función addLists

- La función ***vote*** es pública y se encarga de almacenar los votos de cada elector, por lo tanto, actualiza el número de votos de cada lista y realiza la verificación de voto único en base a la cédula, figura 4.3.

```
function vote(uint _list, uint _ci) public {
    Voter storage sender = voters[_ci];
    require(!sender.voted, "Already voted.");
    sender.ci = _ci;
    sender.voted = true;
    lists[_list].voteCount += 1;
}
```

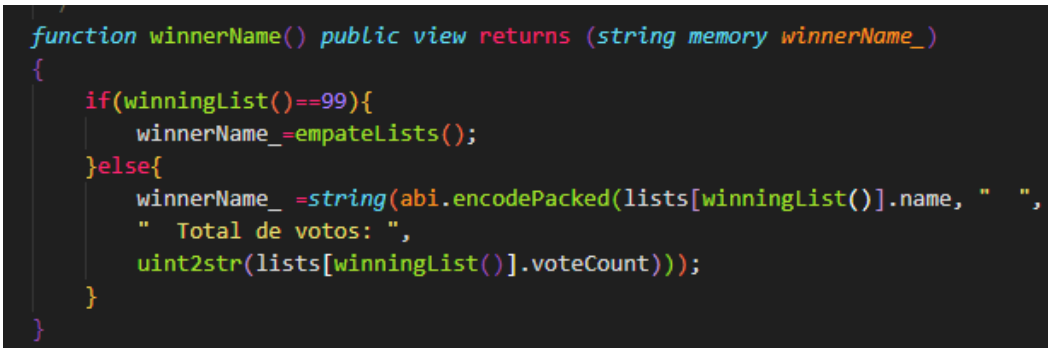
Figura 4.3. Contrato inteligente, función vote

- La función ***winningList*** se encarga de retornar la lista ganadora en base al número de votos obtenidos, también se verifica si existe un empate entre las listas. Esta función es pública, permitiendo el acceso a la información de la lista ganadora al público en general, figura 4.4.

```
function winningList() public view returns (uint winningList_)
{
    uint winningVoteCount = 0;
    for (uint p = 0; p < lists.length; p++) {
        if (lists[p].voteCount > winningVoteCount) {
            winningVoteCount = lists[p].voteCount;
            winningList_ = p;
        }else{
            if (lists[p].voteCount == winningVoteCount) {
            winninList_ = 99;
        }
        }
    }
}
```

Figura 4.4. Contrato inteligente, función winningList

- La función ***winnerName*** es utilizada para mostrar los resultados con la lista ganadora y el número de votos respectivos. Además, realiza una verificación en el caso de encontrar listas con el mismo número de votos, figura 4.5.



```
function winnerName() public view returns (string memory winnerName_)
{
    if(winningList()==99){
        winnerName_=empateLists();
    }else{
        winnerName_ =string(abi.encodePacked(lists[winningList()].name, "   ",
        "  Total de votos: ",
        uint2str(lists[winningList()].voteCount)));
    }
}
```

Figura 4.5. Contrato inteligente, función winnerName

- La función ***getStats*** devuelve el estado de las listas con sus respectivos votos, sin tomar en cuenta la lista ganadora.
- La función ***empateList*** nos devuelve el nombre de las listas que obtuvieron un empate con el número de votos.

Código fuente:

Ingrese en el siguiente repositorio de GitHub para obtener la prueba de concepto realizada con la implementación de Smart Contracts: https://github.com/Alekz23/-Tesis-vote-blockchain-MERN-final

Configuración de la red Polygon en Metamask

1. Ingresamos a la página oficial de Metamask y descargamos el plugin en el navegador de nuestra preferencia siempre y cuando sea compatible.

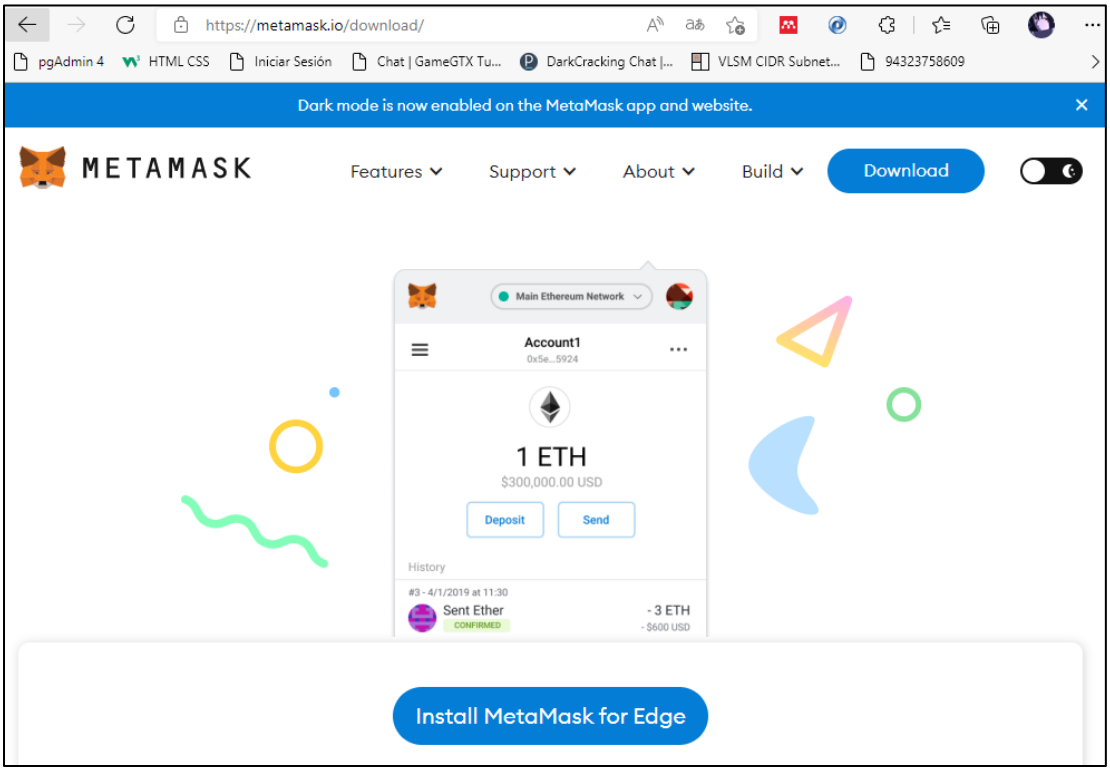


Figura 4.6. Descarga de Metamask

2. En el caso de no disponer de una cuenta Metamask, debemos crear una, una vez creada nos brindara una frase clave con la que podremos ingresar desde cualquier dispositivo.

Figura 4.7. Creación de una cuenta en Metamask

3. En Metamask, podemos agregar la red de pruebas de Polygon haciendo clic en el menú desplegable y seleccionando la opción “Agregar Red”.

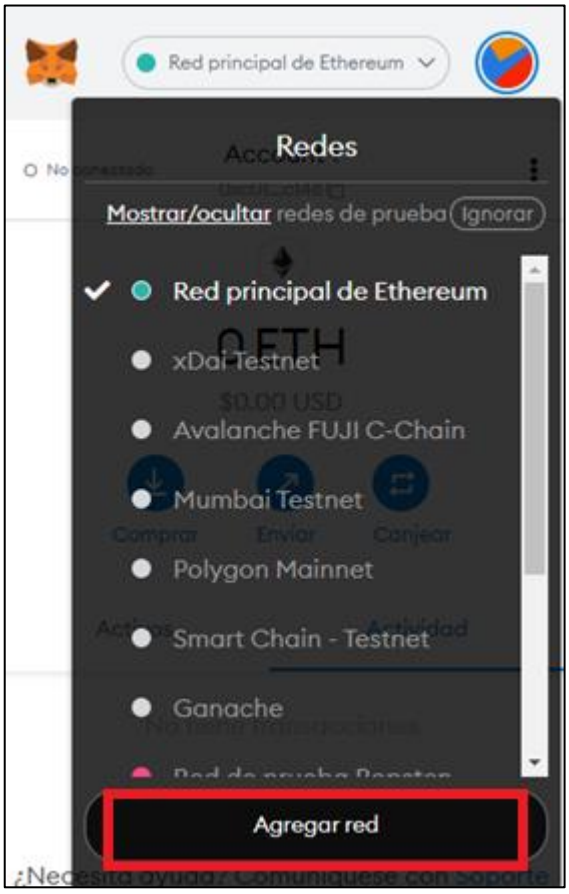


Figura 4.8. Agregar nueva red en Metamask

4. Configuramos la red de Polygon con los siguientes parámetros.

Metamask Network Parameters

Network Name: Mumbai Testnet

New RPC URL: https://rpc-mumbai.maticvigil.com

Chain ID: 80001

Currency Symbol: MATIC

Block Explorer URL: https://polygonscan.com/

Figura 4.9. Configuración de la testnet de Polygon

5. Finalmente, puedes agregar tokens MATIC de prueba para realizar transacciones en la red e interactuar con las funciones de los contratos inteligentes. Puedes conseguir MATIC de prueba ingresando tu dirección de Metamask en el siguiente enlace: https://faucet.polygon.technology/

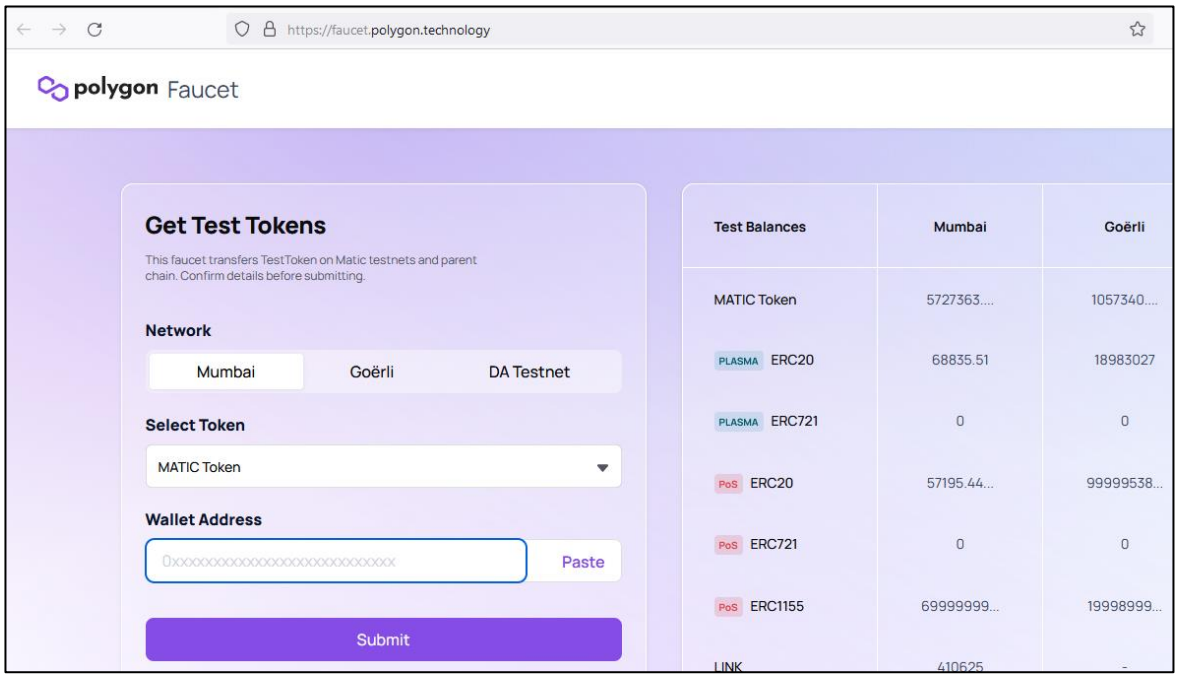


Figura 4.10. Faucet de Polygon