UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE CIENCIAS PURAS Y NATURALES

CARRERA DE INFORMÁTICA

PERFIL DE TESIS DE GRADO

"UN MODELO DE APLICACIÓN DESCENTRALIZADA PARA AUMENTAR LA SEGURIDAD EN PROCESOS ELECTORALES ELECTRÓNICOS USANDO TECNOLOGÍA BLOCKCHAIN"

TESIS PARA OPTAR EL GRADO ACADÉMICO: LICENCIATURA EN INFORMÁTICA
MENCIÓN: INGENIERÍA DE SISTEMAS INFORMÁTICOS

POSTULANTE: ROBERTO CARLOS CHAMBI CALIZAYA

DOCENTE: PH. D. FATIMA DOLZ SALVADOR

TUTOR: LIC. LUCIO TORRICO DIAZ

LA PAZ - BOLIVIA

Junio, 2022

ÍNDICE

1. Título de la tesis **2**
2. Introducción. **2**
3. Área temática **3**
4. Formulación del problema **3**
4.1. Problema central. 3
4.2. Problemas específicos. 4
5. Planteamiento de objetivos. **4**
5.1. Objetivo general. 4
5.2. Objetivos específicos. 4
6. Antecedentes. **4**
7. Alcances y límites de la investigación. **6**
7.1. Alcances 6
7.2. Límites 6
8. Hipótesis **7**
9. Variables **7**
10. Justificación **7**
10.1. Justificación social 7
10.2. Justificación económica 7
10.3. Justificación científica 8
11. Aportes **8**
12. Metodología. **8**
12.1. Metodología de investigación. 8
12.2. Metodología de desarrollo de la aplicación descentralizada. 9
13. Marco teórico **9**
13.1. Blockchain. 9
13.2. Funcionamiento de la Blockchain. 9
13.3. Criptografía en Blockchain. 10
13.4. Contratos inteligentes. 10
13.5. Aplicabilidad de la tecnología Blockchain al voto electrónico. 11
13.6. Aplicaciones descentralizadas (DApps) 11
14. Esquema tentativo **12**
15. Cronograma **15**
16. Referencias **16**
Anexos **18**

1. Título de la tesis

Un modelo de aplicación descentralizada (DApp) para aumentar la seguridad en procesos electorales electrónicos usando tecnología Blockchain.

2. Introducción.

La tecnología Blockchain o cadena de bloques ha surgido a consecuencia del gran éxito que tuvieron las criptomonedas, una moneda electrónica que funciona sin intermediarios y con métodos criptográficos para asegurar las transacciones. Ese éxito desencadenó en múltiples aplicaciones de esta tecnología prometiendo traer incrementos significativos en la eficiencia para el intercambio de información descentralizada y transparente, la Blockchain puede ser integrada en muchas áreas donde se necesite la transparencia y seguridad de datos, como en un sistema de comicios electorales.

La tecnología Blockchain puede ser una solución a la incertidumbre en los procesos electorales gracias a las ventajas que nos ofrece, como: la transparencia, la seguridad criptográfica, seguridad del anonimato, la inmutabilidad de registros una vez estando en la red, menos intermediarios para cada proceso, entre otros (Fernandez, 2020).

Al hacer uso de la tecnología Blockchain en un proceso electoral se debe contemplar el rediseño de las etapas como: el registro de votantes o empadronamiento, presentación de papeletas oficiales con los partidos o frentes habilitados, ejercicio del voto, conteo de votos con asistencia libre y exposición de resultados finales. En cada una de las etapas mencionadas se debe hacer un estudio de factibilidad para poder implementar la tecnología Blockchain a todas las etapas o hacer una combinación usando otras tecnologías. Por ejemplo, el *ejercicio del voto* presenta muchas dificultades desde la perspectiva del votante, como creer que su voto ha sido cambiado o si no fue contado.

Por consiguiente, en esta tesis se profundizará en la aplicación de los lineamientos de la tecnología Blockchain al voto electrónico, mostrando un modelo que considere los procesos que se realizan desde la etapa de emisión de un voto hasta el conteo del mismo, verificando la viabilidad de su aplicación desarrollando una DApp[1] para un caso específico de uso.

3. Área temática

El área temática de esta investigación es la criptografía utilizada en una red Blockchain, ésta garantiza la confiabilidad e inmutabilidad de los datos al momento de circular por la red más insegura, internet.

[1] DApp es una aplicación descentralizada con una cadena de bloques. (BBVA, 2022)

La tecnología Blockchain o cadena de bloques busca efectuar transacciones descentralizadas entre entidades sin la necesidad de que prime la confianza entre estas (Linares, 2021).

Para registrar los bloques de información y para facilitar la recuperación de todos los bloques se usan conceptos criptográficos como algoritmos de clave asimétrica y funciones hash, con esto se consigue que los datos de cada bloque no se puedan alterar.

El área de la criptografía aplicada a las cadenas de bloques es significativamente importante para mantener la seguridad, transparencia e inmutabilidad que tiene la tecnología Blockchain y por consiguiente que heredan las DApps.

4. Formulación del problema

La poca participación en los comicios electorales debido a la pérdida de confianza en dichos procesos, la demora en exposición de resultados y la susceptibilidad a errores en el conteo entre muchos otros problemas condujeron a optar por los sistemas de votación electrónica como una solución para mitigar las dificultades que se tenía en los procesos electorales convencionales, haciendo que varios países apuesten por estos sistemas para su implementación, pero estos también presentaron algunos inconvenientes como la centralización en la etapa de escrutinio, haciéndose vulnerable a la alteración de los votos, esto también a causa del manejo deficiente de los datos en los procesos de emisión del voto. En ese contexto, surge la necesidad de usar una nueva tecnología que garantice la transparencia y descentralización así como la que nos brinda la tecnología Blockchain, sin embargo, el escaso conocimiento del funcionamiento de la tecnología Blockchain aplicada a comicios electorales hace que la desconfianza de las personas aumente en el momento de su implementación.

En términos generales, la tecnología Blockchain brinda seguridad e inmutabilidad a los datos de la red, no obstante, la ejecución de las transacciones realizadas no son visibles ni públicas, eso genera que al momento de hacer una auditoría el sistema de voto electrónico sea considerado como un sistema con transparencia parcial.

4.1. Problema central.

Procesos de voto electrónico convencional con manejo ineficiente de datos, proceso de escrutinio lento, centralizado, con poco nivel de seguridad y transparencia.

4.2. Problemas específicos.

- Poca participación en comicios electorales.

- Sistemas de voto electrónico convencionales vulnerables a alteración de votos, a causa de la centralización y el mal manejo de datos.
- Vulnerabilidad en el conteo de votos.
- Deficiencias en el escrutinio que retarda la etapa de exposición de resultados.
- Conocimiento escaso del funcionamiento de la tecnología Blockchain aplicado a comicios electorales.
- Inexistencia de un registro auditable verificable por el votante.
- Poca transparencia en el proceso y registro de votos.

5. Planteamiento de objetivos.

5.1. Objetivo general.

- Modelar y diseñar una DApp que optimice la seguridad en el manejo de votos mostrando la viabilidad de uso de los protocolos y lineamientos Blockchain para el ejercicio del voto en un proceso electoral.

5.2. Objetivos específicos.

- Expresar el funcionamiento de la tecnología Blockchain aplicado a comicios electorales, mediante un enfoque sistémico para infundir nociones de esta nueva tecnología.
- Modelar las etapas de un proceso de votación enlazando las características de la votación tradicional a los protocolos y lineamientos de la tecnología Blockchain.
- Estructurar el contrato inteligente modelo para la realización de votos.
- Desarrollar una DApp aplicando los mecanismos de validación pertenecientes a la tecnología Blockchain mediante el uso de contratos inteligentes.
- Integrar los módulos de conteo y exposición de votos al modelo del proceso de votación.

6. Antecedentes.

Hasta la fecha todos procesos electorales se realizan con el voto tradicional usando papeletas y ánforas, en Bolivia no se ha establecido ninguna ley o decreto que incorpore referencias a procesos electorales electrónicos. En el ámbito internacional ya existen países que han implementado el voto electrónico entre ellos Estados Unidos desde el año 2001; en Argentina se implementó también el voto electrónico para algunas zonas, al igual que en Perú (La vanguardia, 2017). También existen universidades que han implementado el voto electrónico como la Universidad Nacional de Educación a Distancia y la Universidad Rovira i Virgilli donde usan sus sistemas de votación electrónica para las elecciones de rectorado (González et al., 2010).

En el proceso de investigación se ha encontrado literatura que se asemeja a la investigación de esta tesis, entre las que destacan están:

- En el año 2019, Lucuy, Köller y Galaburda presentan un artículo llamado *Modelo de sistema de votación electrónica aplicando la tecnología de cadena de bloques,* donde muestran un modelo con la arquitectura de la moneda criptográfica bitcoin. Identificando los actores en las etapas de votación crean un flujo para emitir un voto para que éste sea registrado en la red Blockchain. Un voto es considerado como una moneda, a cada votante habilitado se le asigna una moneda para realizar su voto, un candidato tiene una identidad también con una moneda, pero a diferencia de los demás este puede recibir más monedas que llegan a ser los votos a su favor.
- En el año 2020, Di Francesco y Mori presentan un artículo titulado *Blockchain 3.0 Applications Survey*. En el artículo hablan sobre las aplicaciones interesantes que tiene la tecnología Blockchain. Identifica al voto electrónico con Blockchain como un desafío para los atacantes, también indican que debe existir una autoridad central que identifique a los votantes habilitados y de la misma manera que en el artículo anterior, se simula transacciones donde los candidatos reciben monedas (votos) en su cuenta y al finalizar para el conteo se verifica el libro de transacciones para ver quien recibió más votos.
- Recientemente se publicó un artículo en la revista MIJRD por Ali, Iqbal, Hussain, y Younas, M. titulado *An Efficient E-Voting Algorithm and Dapp Using Blockchain Technology* (2020). Dicho artículo muestra el diseño de un sistema seguro de votación usando funciones hash para la criptografía como es común en la tecnología Blockchain, lo más llamativo de este trabajo es el uso de la plataforma Ethereum que es usado para crear programas descentralizados, después de enfrentarse a los retos que presenta el uso de una nueva tecnología se menciona que se pueden añadir otras tecnologías para poder mejorar el diseño realizado.
- Un trabajo con enfoque en las aplicaciones descentralizadas es el presentado por Suárez (2020) que expone una investigación donde analiza las diversas soluciones que la Blockchain nos brinda a problemas con la seguridad, transparencia e inmutabilidad; toma una problemática muy general que es la modificación y acceso de información sensible, desarrolla una DApp con un sistema de permisos inalterables en el que se identifican a usuarios y privilegios para cada uno, afirma que la aplicación puede servir para usos como: informes clínicos privados o datos bancarios.

Existen muchos otros trabajos referentes al voto electrónico con el uso de Blockchain tal es el caso de una tesis recientemente realizada por Fernandéz (2021) donde ofrece una visión aplicativa de su sistema velando por la seguridad, eficiencia y transparencia al momento de la votación. Dejando de

lado el enfoque aplicativo, Sandoval (2021) en su tesis de maestría hace un estudio para la recomendación del voto electrónico usando la tecnología Blockchain, donde menciona que se debe consensuar la democracia participativa y que es necesario que se practique la adopción de esta nueva tecnología, de acuerdo a encuestas realizadas y mediante la aplicación de pruebas estadísticas concluye que la aplicación de la tecnología Blockchain genera más confianza en procesos electorales.

7. Alcances y límites de la investigación.

7.1. Alcances

El alcance que tendrá esta tesis será en base a los objetivos planteados para el desarrollo del mismo, fundamentando la investigación con un enfoque cuantitativo de tipo experimental. La razón principal es porque la Blockchain es un campo muy nuevo, con actividad y conocimiento mínimo en Bolivia; es por eso que esta investigación pretende mostrar la tecnología Blockchain aplicada al voto electrónico y cómo es que éste llegaría a funcionar si se implementara en comicios electorales de cualquier índole.

En la realización de esta tesis se mostrará un modelo con el fin de que en un tiempo futuro se pueda desarrollar e implementar en alguna institución para comicios electorales. El modelo describirá el proceso del ejercicio del voto usando los lineamientos pertenecientes a la tecnología Blockchain con ayuda de los contratos inteligentes.

Para poder mostrar los conceptos criptográficos y lineamientos Blockchain se desarrollará una aplicación descentralizada (DApp) para un caso específico usando una metodología de prototipado que nos permita contemplar un modelo de voto electrónico descentralizado y las características que lo hacen favorable ante los demás sistemas de voto electrónico.

7.2. Límites

Esta tesis se limita al diseño de una aplicación descentralizada para comicios electorales, en instituciones donde se realizan elecciones. La aplicación no será implementada, tampoco se hará un análisis profundo sobre los requerimientos de hardware necesarios para poner en funcionamiento la aplicación, el trabajo se enfocará en el uso de los protocolos de la tecnología Blockchain para obtener mayor seguridad en la emisión del voto y el escrutinio, de igual manera la tesis no presentará un análisis profundo sobre la etapa pre-eleccionaria como el registro o empadronamiento de votantes puesto que esto no forma parte de los objetivos.

En el desarrollo de este trabajo se usará un entorno virtual de una red Blockchain que nos permitirá adecuar las características y requerimientos necesarios para llegar a una aplicación descentralizada apropiada.

8. Hipótesis

H: "Los protocolos de la tecnología Blockchain y la eficiencia de los contratos inteligentes como papeleta de sufragio aplicados en el proceso de registro y conteo de votos le brindan un mayor nivel de seguridad y disminuyen la posibilidad de alteración de los votos electrónicos".

9. Variables

Variable dependiente.

Nivel de seguridad en la transmisión de un dato.

Variables Independientes.

- Aplicación de protocolos Blockchain.
- Eficacia de los contratos inteligentes.

10. Justificación

10.1. Justificación social

La tecnología ha logrado satisfacer las necesidades básicas de la sociedad como con la comunicación a distancia con las aplicaciones de videollamadas. Haciendo cada vez más sencillas las actividades diarias del ser humano.

La adaptación de nuevas tecnologías a los procesos electorales cambia la idea tradicional respecto al ejercicio de la democracia, esto conduce a la sociedad al camino del desarrollo tecnológico; con el uso de los protocolos de la tecnología Blockchain se asegura de que en el ejercicio de la democracia todo voto sea respetado.

10.2. Justificación económica

Los procesos electorales emplean presupuestos altos para gastos en desplazamiento de personal y gastos en logística. Estos gastos se vuelven a repetir para cada proceso electoral, con la implementación de un sistema de voto electrónico descentralizado los gastos se reducen para procesos electorales posteriores, puesto que el sistema no es desechable cuando está bien diseñado y estructurado.

10.3. Justificación científica

La tecnología Blockchain ya es un avance tecnológico sustancial, sus diferentes aplicaciones pueden ahorrar tiempo y dinero, los algoritmos criptográficos que usan los protocolos Blockchain se pueden aplicar a comicios electorales, esto de alguna manera es una transformación en la manera de votar y una evolución en las diversas aplicaciones que tiene la tecnología Blockchain.

El desarrollo de las aplicaciones descentralizadas (DApps) para nuevos usos cambian el rostro de la informática y trascienden a un nuevo campo de desarrollo de aplicaciones lo que hace que la informática amplíe su contribución a la revolución digital y tecnológica.

11. Aportes

- La tesis tiene como aporte principal la divulgación de la tecnología Blockchain aplicada al voto electrónico y cómo es que funcionan los lineamientos y protocolos Blockchain para hacer que los registros guardados en un bloque sean inmutables.
- Como aporte secundario, brindar una glosa sobre la viabilidad de la aplicación de conceptos criptográficos y lineamientos de la tecnología Blockchain y si se pueden mejorar algunos aspectos para trabajos futuros.
- El desarrollo de una DApp muestra un criterio de la adaptación de una metodología de desarrollo ágil para el campo de desarrollo de una aplicación descentralizada.

12. Metodología.

12.1. Metodología de investigación.

El término metodología hace referencia al conjunto de métodos que se siguen en una investigación ya sea científica o social (Landeau, 2007). Considerando el objetivo de esta tesis se optó por usar la metodología de investigación tecnológica. Siguiendo un diseño de investigación cuantitativa de tipo experimental. Espinoza (2010) nos indica que para iniciar la investigación es necesaria una planificación, ésta consta de los siguientes pasos:

A. Definición del problema
   - Reconocimiento de hechos
   - Descubrimiento del problema
   - Formulación del problema
B. Formulación teórica.
C. Construcción del modelo teórico.
   - Selección de factores pertinentes

- Intervención de la hipótesis y suposiciones auxiliares

D. Diseño experimental.
   - Pre-experimental
   - Cuasi-experimental
   - Experimental

E. Prueba de Hipótesis
   - Diseño de la prueba
   - Ejecución de la prueba
   - Elaboración de datos
   - Inferencia de la conclusión

F. Conclusiones.

12.2. Metodología de desarrollo de la aplicación descentralizada.

Una aplicación descentralizada no tiene las mismas características que una aplicación tradicional en cuanto al desarrollo, el campo de las aplicaciones descentralizadas sigue siendo algo nuevo y no cuenta con una estructura de desarrollo bien definida. Por dichas razones en esta tesis se hará uso de la metodología de prototipos o modelo de desarrollo evolutivo, misma que según (EcuRed, 2019) cuenta con las siguientes etapas:

A. Recolección y refinamiento de requisitos.
B. Modelado y diseño rápido
C. Construcción del prototipo
D. Desarrollo y evaluación
E. Refinamiento del prototipo
F. Producto de ingeniería

13. Marco teórico

13.1. Blockchain.

La Blockchain que traducido al español significa cadena de bloques, es una tecnología revolucionaria de la red internet, también es conocido como, “un libro de contabilidad compartido e inmutable que facilita el proceso y registro de transacciones y seguimiento de activos de una red empresarial” (Gupta, 2018) a causa del gran impacto de la criptomoneda Bitcoin.

Más allá de las definiciones que ha adoptado esta tecnología, la Blockchain es una base de datos que almacena cada operación o transacción realizada, los datos almacenados se comparten con todos los

nodos[2] participantes de la red (es por eso que también a la Blockchain se le denomina una base de datos distribuida).

13.2. Funcionamiento de la Blockchain.

Las operaciones o transacciones almacenadas están encadenadas unas a otras de manera ordenada, es ahí donde nace el término de 'bloque', que es donde se guardan éstas transacciones, cada bloque está constituido por tres elementos importantes: un código alfanumérico generado por un conjunto de funciones hash de criptografía (Simoes, 2022) que enlaza el bloque actual con el bloque anterior, el contenido de la transacción confirmada y otro código alfanumérico creado por un conjunto de funciones hash de criptografía que es el enlace a un nuevo bloque que será creado cuando exista una nueva transacción. No obstante, la tecnología Blockchain no sólo se limita a eso, pues "para mantener la integridad de la cadena de bloques y evitar estos ataques Sybil[3], se trabaja con el protocolo PoW[4] (Proof-of-Work), con el que identificamos otra propiedad de Blockchain: el protocolo de consenso" (Linares, 2021). Dicha propiedad consiste en mandar una tarea compleja de cómputo a una entidad que quiere insertar un nuevo bloque con una transacción u operación que modifique nuestro libro de registros, la respuesta de esta entidad es verificada por los nodos de la red, quienes indican si la respuesta es correcta o incorrecta, si la respuesta es correcta la nueva transacción es añadida a continuación del último bloque, caso contrario se rechaza al bloque y nuestra cadena permanece intacta. Pero, ¿Quién es la entidad que resuelve la tarea compleja de cómputo? Pues esas entidades son denominadas validadores, aunque en la terminología de las criptomonedas son llamados 'mineros'; "los mineros utilizan la potencia informática (hash) para procesar transacciones y obtener recompensas" (S. J., 2022). La respuesta que deben encontrar los 'mineros' es el código alfanumérico hash que tiene el último bloque, para así poder enlazar la transacción que se realizó.

13.3. Criptografía en Blockchain.

En la tecnología Blockchain comúnmente se utilizan dos tipos de algoritmos criptográficos: los algoritmos de clave asimétrica y funciones hash.

---

[2] En una cadena de bloques, un **nodo** suele ser un dispositivo como una computadora, computadora portátil o servidor. (Blockchain Media, 2021)

[3] Un ataque Sybil ocurre cuando en un sistema distribuido se infiltra una entidad que crea identidades falsas o controla varias identidades de la red. (Binance Academy, 2021)

[4] PoW es una prueba de trabajo consiste en que un cliente (ordenador) realice complejas operaciones de cómputo para que después sea verificado por la red. (Bit2me Academy, 2022)

La criptografía de clave asimétrica también es conocida como clave pública, emplea dos llaves diferentes en cada uno de los extremos de la comunicación para cifrarla y descifrarla. Cada usuario de la comunicación tendrá una clave pública y otra privada. (López, 2022)

Una función criptográfica hash es un algoritmo matemático que transforma cualquier dato entrante en una serie de caracteres de salida, con una longitud fija o variable, dependiendo del algoritmo hash que estemos utilizando. (López, 2021)

13.4. Contratos inteligentes.

Los contratos inteligentes también conocidos como *Smart Contracts* son códigos informáticos escritos en un lenguaje de programación, están almacenados en una red Blockchain y tienen sentencias escritas de acuerdo al uso que se requiera dar. Estos contratos funcionan sin la necesidad de una autoridad que pueda dar fe de la validez del contrato, pues solo se necesita a las dos partes para cerrar el contrato y éste queda en la red Blockchain sin que ninguna de las partes pueda negar el acuerdo. De esta manera el contrato inteligente se vuelve inmutable y transparente.

Cabe resaltar, que "un contrato inteligente puede ser creado y llamado por por personas físicas y/o jurídicas. Pero también por máquinas y otros programas que funcionan de manera autónoma" (Bit2Me Academy, 2022).

13.5. Aplicabilidad de la tecnología Blockchain al voto electrónico.

Todo lo mencionado en puntos anteriores es lo que hace a la tecnología Blockchain inmutable y transparente en cuanto a los registros que guarda en su red; de tal manera que se ha dado a conocer una diversidad de aplicaciones que se puede conseguir con los protocolos pertenecientes a la tecnología Blockchain, una aplicación entre todas es la solución al manejo de los votos ineficientes y poco seguros que usan los sistemas de voto electrónico; en muchos artículos indican la posibilidad de esa solución, como Benjamin Yahari que indica que "La Blockchain puede ser una solución ya que permitiría un sistema de voto en el que las identidades de los votantes estuviesen protegidas, sean infalsificables y a un coste prácticamente nulo y de acceso público" (Yahari, 2017).

13.6. Aplicaciones descentralizadas (DApps)

Una aplicación descentralizada es una categoría especial que funciona a base de una red descentralizada (Hurtado, 2022), una DApp comparte las características de una Blockchain ya que se originó de esta tecnología gracias a los smart contracts que funcionan como un contrato sin ningún intermediario que interceda en la transacción. "De la misma manera que en cualquier sistema

con tecnología Blockchain las técnicas de encriptación proporcionan una gran seguridad. Gracias a ello, la información sensible de los usuarios se blinda frente a robos, manipulación o ataques informáticos por parte de terceros, ya que no existe de forma centralizada en ninguna base de datos" (BBVA, 2022).

14. Esquema tentativo

RESUMEN

INTRODUCCIÓN

CAPÍTULO I

MARCO REFERENCIAL

1.1. Formulación del problema

1.1.1 Problema central

1.1.2 Problemas específicos

1.2. Planteamiento de objetivos

1.2.1. Objetivo central

1.2.2. Objetivos específicos

1.3. Hipótesis

1.4. Alcances y limitaciones

CAPÍTULO II

MARCO TEÓRICO

2.1. Blockchain

2.1.1. Componentes de Blockchain

2.1.1.1. Nodos

2.1.1.2. Mineros o Validadores

2.1.1.3. Bloques

2.1.1.4. Transacciones

2.1.2. Algoritmos de consenso

2.1.2.1. Proof of Work

2.1.2.2. Proof of Stake

2.1.3. Algoritmos criptográficos

2.1.3.1. Algoritmos simétricos

2.1.3.2. Algoritmos asimétricos

2.1.3.3. Hash

2.1.4. Tipos de Blockchain

2.1.4.1. Blockchain privados

2.1.4.2. Blockchain público

2.1.4.3. Blockchain mixto

2.2. Ethereum y la Web3

2.2.1. ¿Qué es Ethereum?

2.2.2. Plataformas similares a Ethereum

2.3. Smart Contract

2.4. Aplicaciones descentralizadas (DApps)

2.4.1. Ventajas

2.4.2. Diferencias entre una aplicación descentralizada y una tradicional

2.4.3. Niveles de una DApp

2.5. Voto electrónico

2.5.1. Características de validez del voto electrónico

CAPÍTULO III

MARCO APLICATIVO

3.1. Funcionamiento del proceso de votación con Blockchain

3.2. Modelado de las etapas del voto electrónico

3.2.1. Actores

3.2.1.1. Proceso electoral tradicional

3.2.1.2. Proceso electoral electrónico

3.2.1.3. Proceso electoral electrónico aplicando la tecnología Blockchain

3.2.2. Procesos

3.2.2.1. Identificación

3.2.2.2. Emisión del voto

3.2.2.3. Depósito del voto en la urna electoral

3.2.3.4. Registro de participación

3.2.3. Relaciones y flujos

3.2.4. Modelo

3.3. Herramientas tecnológicas

3.4. Definición de las funcionalidades de la aplicación

3.4.1. Recolección de requisitos

3.5. Desarrollo de la aplicación descentralizada

3.5.1. Diseño y modelado
3.5.2. Construcción de los módulos necesarios
3.5.3. Evaluación
3.5.4. Refinamiento
3.5.5. Producto de la re-ingeniería

CAPÍTULO IV

MARCO EXPERIMENTAL

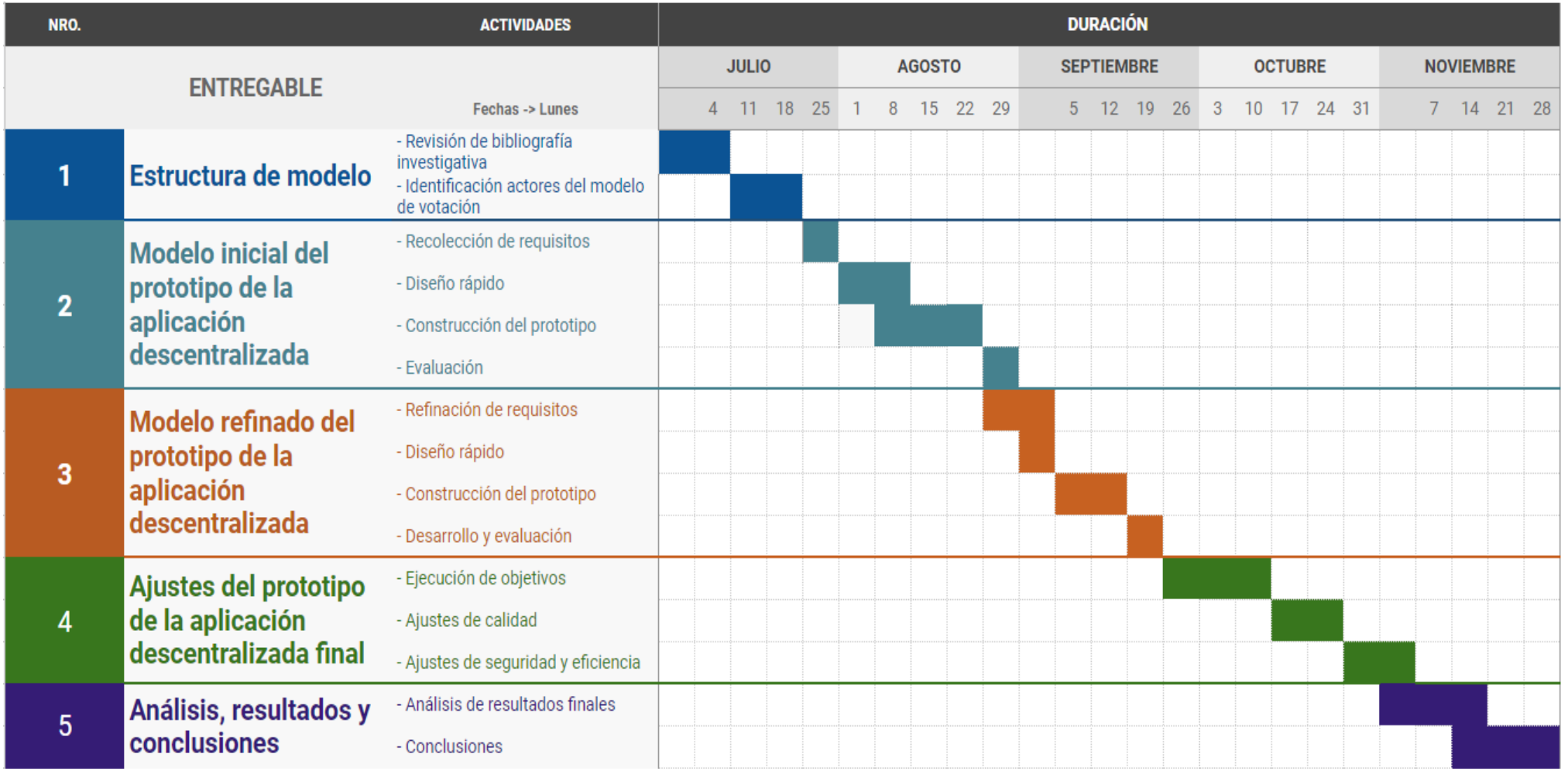
4.1. Introducción
4.2. Definición del problema
4.3. Ambiente de desarrollo experimental
4.3.1. Objeto de experimento
4.3.2. Datos con los que se trabajará
4.4. Diseño experimental
4.5. Resultados experimentales
4.6. Análisis de resultados
4.7. Evaluación
4.8. Discusión

CAPÍTULO V

MARCO CONCLUSIVO

5.1. Estado de objetivos
5.1.1 Análisis de las variables
5.3. Conclusiones
5.3.1. Aportes de los beneficios aplicativos de una DApp
5.4. Recomendaciones
5.4.1. Viabilidad de uso en una institución
5.4.2. Gobernanza que beneficia a una aplicación descentralizada
5.5. Futuros trabajos y nuevos retos
BIBLIOGRAFÍA
REFERENCIAS
ANEXOS

15. Cronograma



16. Referencias

Ali, B., Iqbal, F., Hussain, I., & Younas, M. (2022). *An Efficient E-Voting Algorithm and Dapp Using Blockchain Technology*. https://www.mijrd.com/papers/v1/i3/MIJRDV1I30008.pdf

BBVA. (2022, marzo 29). *¿Qué son las DApps y por qué serán cada vez más importantes?* BBVA. https://www.bbva.com/es/que-son-las-dapps-y-por-que-seran-cada-vez-mas-importantes/

Binance Academy. (2021, octubre 4). *Ataques de Sybil*. https://academy.binance.com/es/articles/sybil-attacks-explained

Bit2me Academy. (2022, marzo 23). *¿Qué es prueba de trabajo / Proof of Work (PoW)?* https://academy.bit2me.com/que-es-proof-of-work-pow/

Bit2Me Academy. (2022, junio 07). *Smart Contracts: ¿Qué son, cómo funcionan y qué aportan?* Bit2Me Academy. https://academy.bit2me.com/que-son-los-smart-contracts/

Blockchain Media. (2021, septiembre 1). *¿Qué son los nodos Blockchain y Bitcoin?* https://Blockchain-media.org/es/chto-takoe-Blockchain-i-node-bitcoin/

Di Francesco, D., & Morib, P. (2020). *Blockchain 3.0 Applications Survey*. *1*. http://webhost.services.iit.cnr.it/staff/paolo.mori/reprint_Blockchain_3.0_survey_2020.pdf

EcuRed. (2019, agosto 29). *Modelo de prototipos*. https://www.ecured.cu/Modelo_de_prototipos

Espinoza, C. (2010). *Metodología de investigación tecnológica* (1st ed.). Imagen Gráfica SAC.

Fernandez, C. (2020, septiembre 10). *Cómo Blockchain puede cambiar la forma en que votamos*. BBVA. https://www.bbva.com/es/como-Blockchain-puede-cambiar-la-forma-en-que-votamos/

Fernández, C. (2021). *Sistema de votación electrónica usando tecnología Blockchain para procesos electorales*. [Tesis de licenciatura]. Universidad Mayor de San Andrés

Giménez, S. (2021). *Las criptomonedas, el Blockchain y su comparativa con las divisas*. Repositorio institucional de la Universidad de Zaragoza. https://zaguan.unizar.es/record/100930

González, A., Alfonz, L., & Bordas, M. (2010). *Voto electrónico vinculante en la Universidad Rovira i Virgilli. Dialnet*. https://dialnet.unirioja.es/servlet/articulo?codigo=3252129

Gupta, M. (2018). *Blockchain for Dummies*. John Wiley & Sons, Incorporated.

Hurtado, J. S. (2022, febrero 28). *¿Qué son las DApps o Aplicaciones Descentralizadas?* IEBS. https://www.iebschool.com/blog/dapps-o-aplicaciones-descentralizadas-que-son-y-como-funcionan-finanzas/

Landeau, R. (2007). *Elaboración de trabajos de investigación*.

La vanguardia. (2017, marzo 11). *¿Qué países utilizan ya el voto electrónico?* La Vanguardia. https://www.lavanguardia.com/internacional/20170309/42670140542/paises-utilizan-voto-electronico.html

Linares, M. (2021). Trazabilidad con Blockchain. *CIIS Congreso internacional de Ingeniería de Sistemas*. https://revistas.ulima.edu.pe/index.php/CIIS/article/download/5482/5185

López, A. (2021, Abril 18). *Algoritmos HASH: Qué son, seguridad, uso y funcionamiento*. Redes Zone. https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-hash/

López, A. (2022, Mayo 19). *Criptografía: Algoritmos de clave simétrica y asimétrica explicados*. Redes Zone. https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/

Lucuy, G., Köller, S., & Galaburda, Y. (2019). Modelo de sistema de votación electrónica aplicando la tecnología de cadena de bloques. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1683-07892019000200006

S, J. (2022, Mayo 14). *¿En qué consiste la minería de criptomonedas y qué usos tiene? Te lo explicamos*. Economía 3. https://economia3.com/que-es-mineria-criptomonedas-y-que-usos-tiene/

Sandoval, S. (2021). Estudio para la recomendación del voto electrónico usando tecnología Blockchain en las elecciones seccionales de la ciudad de Guayaquil.

Sheer, F., Gioulis, A., Naeem, R., & Markantonakis, K. (2016). E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy. *[Artículo, Universidad de Londres]*. https://pure.royalholloway.ac.uk/portal/files/30410016/e_voting_Blockchain_2.pdf

Simoes, C. (2022, marzo 24). *¿Qué es la criptografía? ¿Cuál es su papel en Blockchain?* ITDO. https://www.itdo.com/blog/que-es-la-criptografia-cual-es-su-papel-en-Blockchain/

Suaréz, M. (2020). *Desarrollo de aplicación descentralizada con Blockchain: DApp para el acceso y modificación de información sensible.* UOC. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/106746/2/msuareztaTFM0120memoria.pdf

Yahari, B. (2017). Blockchain y sus aplicaciones. *Universidad Católica Nuestra Señora de la Asunción*. http://jeuazarru.com/wp-content/uploads/2017/11/Blockchain.pdf

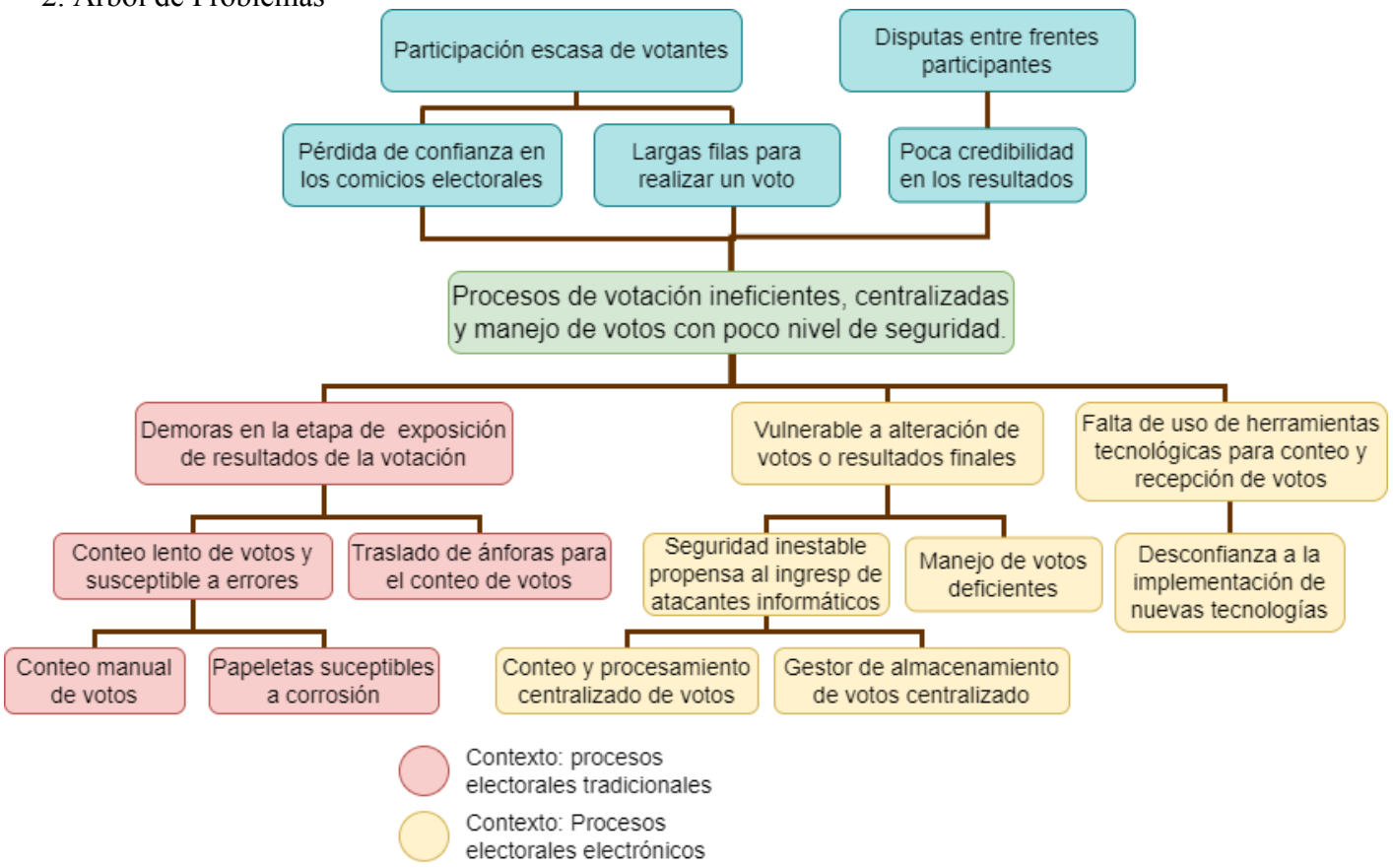
ANEXOS

ANÁLISIS DE SITUACIÓN

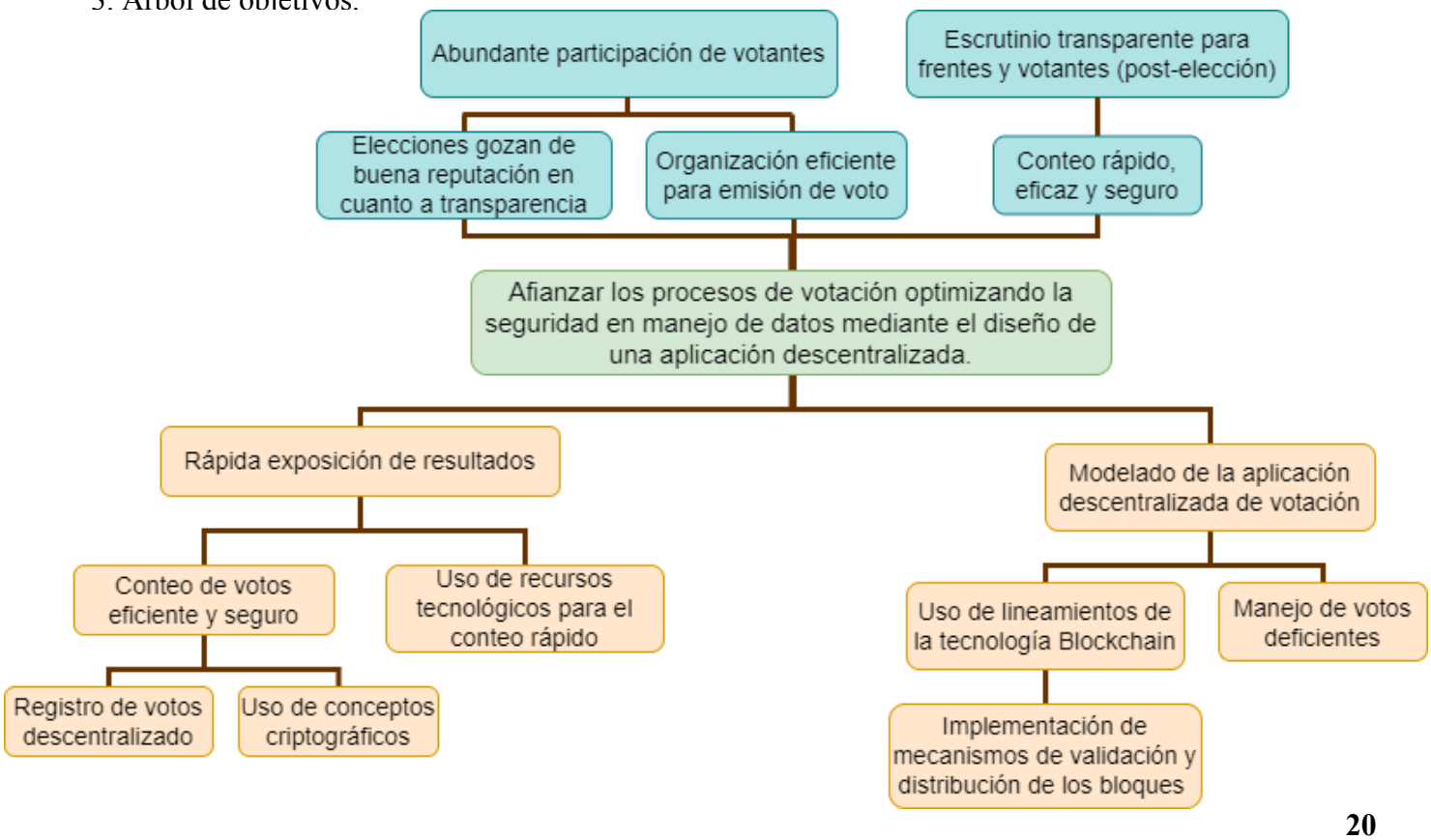
1. Cuadro de involucrados

GRUPOS	INTERESES	PROBLEMAS PERCIBIDOS	RECURSOS Y MANDATOS
VOTANTES	Contar con la seguridad y transparencia en el conteo de votos. Mejorar la duración para realizar el voto.	Desinterés en participar en comicios electorales. Dificultad en conocer los resultados finales con eficacia.	- Resoluciones - Reglamento electoral votantes, jurados de mesa.
FRENTES	Contar con la seguridad y transparencia en el conteo de votos.	Dificultad en conocer los resultados de manera exclusiva. Susceptibilidad a los resultados expresados en el conteo final.	- Resoluciones convocatoria - Reglamento electoral frentes.
COMISIÓN ELECTORAL ORGANIZADORES	Disponer de un instrumento que permita agilizar el proceso de votación. Reducir los gastos en logística. Aumentar la participación en los comicios electorales.	Despliegue de varias personas para realizar los procesos de conteo y distribución de ánforas.	- Resoluciones convocatoria - Listas de frentes habilitados - Lista de votantes habilitados + Presupuesto económico para las elecciones.

2. Árbol de Problemas



3. Árbol de obietivos.



Matriz del marco lógico.

Procesos de elecciones electrónicas transparentes en cada una de las etapas de votación.	Reducción de costos después de implementar el modelo de votación en varias ocasiones.	Informes económicos de gestión de la institución que aplicó la votación electrónica en sus comicios electorales.	El prototipo es implementado en una institución para comicios electorales en distintas ocasiones.
Afianzar los procesos de votación electrónica optimizando la seguridad en el manejo de datos electorales mediante el diseño de un prototipo de red Blockchain.	Un prototipo del proceso de votación usando la tecnología blockchain en funcionamiento para el 30 de noviembre del 2022.	Reporte de inspección del funcionamiento del prototipo en un caso particular.	Los procesos electorales gozan de seguridad al momento de realizar los votos y posteriormente en el escrutinio.
C-1. Modelo del funcionamiento de los procesos de votación usando lineamientos de la tecnología Blockchain. **C-2.** Prototipo aplicando mecanismos de los contratos inteligentes pertenecientes a la tecnología Blockchain. **C-3.** Modelo seguro de exposición de resultados preliminares en una aplicación descentralizada.	Un modelo construido que explica con claridad cómo funciona el proceso de votación aplicando la tecnología blockchain hasta el 25 de noviembre. Componentes de la aplicación descentralizada integrados hasta el 29 de noviembre, cumpliendo con la finalidad de manejo de votos con seguridad y eficacia. Un modelo de exposición de resultados en la aplicación descentralizada construido en su totalidad entre el 25 y 30 de octubre del 2022.	- Informes sobre el avance del desarrollo del modelo de votación electrónica. - Informes de avance del desarrollo del prototipo del modelo. - Informes sobre el avance del modelo de exposición de resultados de los votos.	Los componentes del modelo de voto electrónico se integran de manera satisfactoria con la aplicación de lineamientos blockchain para la realización del voto.

<table>
<tr>
<td>C-1.
- Construcción del módulo de recepción de votos aplicando conceptos criptográficos.
- Construcción del módulo de escrutinio de votos con el uso de la red blockchain.
- Construcción del módulo que resguarde la integridad de los votos mediante el cifrado.
C-2.
- Revisión bibliográfica del funcionamiento a profundidad de la tecnología blockchain.
- Identificar e integrar en el prototipo del modelo a los actores que participan en los comicios electorales.
- Integrar los conceptos de validación de un bloque en la realización de un voto.
C-3.
- Diseño del módulo de conteo para la exposición de votos, usando técnicas criptográficas.
- Diseño del módulo encargado de exponer los resultados en un portal web.</td>
<td>- Para la construcción del prototipo de votación y exposición de conteo de votos es necesario al menos 2 programadores especialistas en Blockchain, estimando 2 meses de trabajo, los honorarios aproximados totales ascienden a Bs. 40000.

<table>
<tr><th>Detalle</th><th>Tiempo</th><th>Monto Bs.</th></tr>
<tr><td>Ingeniero de software</td><td>3 meses</td><td>7000</td></tr>
<tr><td>2 Programadores Blockchain</td><td>2 meses</td><td>40000</td></tr>
<tr><td></td><td>Total</td><td>47000</td></tr>
</table>
</td>
<td>- Informes y reporte de avance de la construcción de los módulos del modelo.

- Informes y pequeñas pruebas de funcionamiento a los módulos del prototipo.

- Informes y reportes concretos sobre el módulo de conteo y exposición de votos.</td>
<td>- Los conceptos criptográficos se aplican acorde a las necesidades para el manejo y conteo de votos.

- Los actores en cada proceso electoral son clasificados en grupos comunes lo que facilita la identificación e integración en el modelo.

- El módulo de conteo puede ser integrado fácilmente en un portal web sin que se pueda modificar los resultados expuestos.</td>
</tr>
</table>