

# Propuesta de diseño de una DApp de Votación Digital para la comunidad del Instituto Politécnico Nacional utilizando Blockchain y Smart Contracts

## Trabajo Terminal No. 1

*Alumnos: Gutiérrez De La Luz Carlos, \*Hernandez Tesillos Irving Rodrigo, Ramírez Arellano Erick Eduardo*

*Director: Erick Eugenio Linares Vallejo*

*\*ihernandezt1502@alumno.ipn.mx*

**Resumen** – El presente trabajo terminal consiste en desarrollar una propuesta de diseño de una DApp (Aplicación Descentralizada) de Votación Digital para la Escuela Superior de Cómputo, con la principal característica de mejorar la confianza, seguridad y eficiencia de elecciones dentro de la comunidad, esto con la ayuda de la tecnología Blockchain, ya que para el uso de criptomonedas le ha permitido explorar sus capacidades en sistemas comerciales, existiendo a través de transacciones almacenadas en cadenas de bloques con datos encriptados y con la ayuda de Smart Contracts que se ejecutan automáticamente acelerando el proceso y definiendo condiciones para el servicio.

**Palabras Clave** – Blockchain, Cadena de bloques, Criptomonedas, DApp, Smart Contracts, Votación Digital.

## 1. Introducción

El Blockchain es un conjunto de tecnologías que ayudan a la transferencia de un valor de un lugar a otro sin intervención de terceros [1]. El Blockchain estipula un nuevo modelo en el que la autenticidad no la verifica un alguien más sino la red de nodos que participa en ello. De ahí que ninguna transferencia de valor se efectúe por medio de un intermediario, sino a través de un consenso, permitiendo almacenar la información en todo momento de manera transparente [1].

Blockchain es una cadena de bloques, los cuales contienen información codificada de una transacción en la red. Y, al estar entrelazados, permiten la transferencia de datos con una codificación bastante segura a través del uso de criptografía [1]. La transferencia no exige un tercero que certifique la información, sino que está distribuida en múltiples nodos independientes e iguales entre sí que la examinan y la validan sin necesidad de que se conozcan entre ellos [1].

Una vez introducida, la información no puede ser eliminada, sólo se podrá añadir nueva información, ya que los bloques están conectados entre sí a través de cifrado criptográfico, por lo que modificar datos de un bloque anterior a la cadena resulta imposible, ya que se tendría que modificar la información de los bloques anteriores [1].

Ahora bien, es importante adentrarnos a conocer sobre los contratos inteligentes o por su término en inglés, Smart Contracts siendo este un mecanismo automático de ejecución de instrucciones informáticas, el cual se utiliza para ejecutar contratos previamente confeccionados por el usuario de forma automática en un entorno que emplee una tecnología de registro distribuido, de ahí su relación con las cadenas de Blockchain [2].

El principal funcionamiento de un Smart Contracts es reducir la necesidad de terceros al procesar y ejecutar de forma autónoma una serie de protocolos informáticos. La ausencia de la intervención humana trae consigo una cadena de ventajas como son el ahorro elevado de costos, protección amplia de la información de interés del usuario y fluidez a la hora de desarrollar las funciones especificadas [3].

Una aplicación descentralizada o DApp son aquellas aplicaciones que no se ejecutan en un entorno centralizado, es decir, que en este tipo de aplicaciones no existe un único nodo central, por lo tanto, puede ser ejecutado en cualquier nodo que forme parte de la red teniendo, así como ventaja una mayor tolerancia a fallos, y la alta disponibilidad y redundancia de los servicios junto con los datos que se obtienen [4].

Otra ventaja que se puede ver reflejada en el uso de aplicaciones descentralizadas es la eliminación de intermediarios, así como la seguridad que ofrece, esto mediante el uso de certificados con claves públicas o privadas y las cadenas de bloque garantizando la autenticidad e integridad de los datos, de ahí su relación y por qué se hace uso con respecto al Blockchain [4].

De acuerdo con la Real Academia Española, se define como votación “Acción y efecto de votar” [5] a lo que votar significa “Dicho de una persona: Dar su voto o decir su dictamen en una reunión o cuerpo deliberante, o en una elección de personas” [6] y digital como “Dicho de un dispositivo o sistema: Que crea, presenta, transporta o almacena información mediante la combinación de bits” [7]. Por lo tanto, se puede definir como votación digital a la acción de emitir un voto mediante el uso de un dispositivo el cual será transportado y almacenado mediante la combinación de bits.

Hoy en día es importante mencionar que los sistemas de votación utilizados en el Instituto Politécnico Nacional han sufrido cambios a lo largo de estos últimos tres años, hablando desde la situación de la Escuela Superior de Cómputo en el año 2020 antes de la presencia del SARS-CoV-2 (COVID-19) las votaciones se realizaban mediante el uso de urnas y plantillas, aunado a esto, se observaba falta de participación por parte de la comunidad de la ESCOM esto debido a la falta de difusión y la importancia que esta merecía. No fue sino hasta después de la presencia de la enfermedad mencionada anteriormente que el sistema de votación se vio en la necesidad de tener una actualización, implementando el Sistema Institucional de Votación Electrónica (SIVE) el cual garantiza que este sistema tenga una alta disponibilidad, seguridad y confiabilidad; no obstante consideramos que tiene áreas de oportunidad que podemos mejorar siendo una de estas la difusión en cada instituto perteneciente al IPN y además, el implementar tecnología Blockchain convertirá el sistema centralizado en descentralizados, por lo tanto, la información no podría modificarse por ninguna persona ya que cada voto quedará registrado en una cadena de bloques haciendo irrefutable la información recibida.

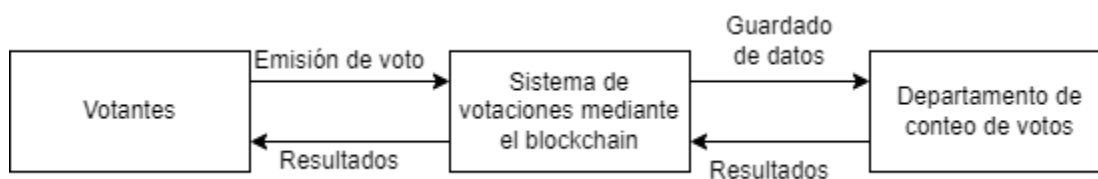
La implementación de este tipo de votaciones digitales no es reciente y es por eso que es necesario analizar cada una de las propuestas más significativas, así como su descripción y conocimiento de las tecnologías que emplean, como se puede observar en la siguiente tabla (Tabla 1).

Nombre del Sistema	Descripción	¿Cuenta con el uso de alguna tecnología?
Vota Fácil	Es un sitio web que permite a los usuarios resolver aspectos básicos para realizar unas elecciones libres y transparentes.	Utiliza como medio de difusión un sitio web donde se encontrarán herramientas básicas para la realización y planeación de eventos electorales [8].
SaberVotar	Herramienta de consulta electoral dedicada a conocer a los candidatos a los distintos cargos de elección popular.	Utiliza un sitio web para realizar las consultas y una base de datos donde reside la información de cada candidato [9].
Voto extranjero	Sistema de voto electrónico por internet que ayuda a que las y los mexicanos residentes en el extranjero puedan participar en las elecciones del país de origen (México).	Hace uso de un sitio web donde se registra al usuario y otro donde se hace seguimiento a la solicitud y una base de datos para almacenar a los usuarios, así como los candidatos a votar [10].
Formulario de Google	Recurso web que ayuda con la elaboración y desarrollo de instrumentos como encuestas, con el objetivo de recabar información de un grupo de personas, así como	Realiza baterías de preguntas en diferentes formatos (texto, listas, opciones) con la facilidad de compartirse mediante un link. De igual forma hace la recolección de

	informes estadísticos o de investigación.	los datos mediante una hoja de cálculo para la realización de gráficos estadísticos [11].
Appsamblea	Es un sistema de votación online en el cual se puede votar desde cualquier lugar del mundo y está enfocado en organizaciones tales como empresas, Asociaciones, Entidades Públicas, Clubes Deportivos, o colectivos de cualquier tamaño	La organización solo tiene que enviar un Excel con la información de las personas participantes y la herramienta gestiona el resto [12].
DEMOKRATIAN	“Es una aplicación web que permite realizar distintos tipos de votaciones online. Es una herramienta que permite a distintos colectivos sociales y partidos políticos realizar consultas entre sus asociados y/o simpatizantes de una forma sencilla.”	Utiliza MySQL, Apache, PHP y cuenta con licencia GNU Affero General Public License que garantiza a los usuarios finales la libertad de usar, estudiar, compartir y modificar el software [13].
“Sistema de Votación electrónica con autenticación Biométrica para ESCOM”	Es un sistema de voto electrónico que pueda avalar la legitimidad y autenticación de los usuarios durante los ejercicios electorales dentro de la ESCOM.	Java SE, JavaFX, MySQL, Lector de huellas DigitalPersona, además de una Impresora térmica, y un servidor y diferentes algoritmos como RSA y SHA-2 [14].
Sistema Institucional de Votación Electrónica (SIVE)	Es un sistema de votación realizada por el Centro Nacional de Cálculo, contando con las características de alta disponibilidad, seguro, robusto y confiable [15].	Sin información.

Tabla 1. Resumen de productos similares Fuente [Elaboración Propia].

A continuación, mostramos el diagrama de contexto de nuestra aplicación, en el cual encontramos tres actores principales, que son los votantes, el sistema de votación y el departamento de conteo de votos:



**Figura 1:** Diagrama de contexto

## 2. Objetivo

Desarrollar un DApp (Aplicación Descentralizada), que permita realizar votaciones electrónicas dentro de la comunidad del Instituto Politécnico Nacional (IPN); facilitando la toma de decisiones de manera confiable y rápida.

### 2.1 Objetivos Específicos

- Implementar el uso del Blockchain en un sistema de votaciones.
- Facilitar la toma de decisiones dentro de la comunidad del IPN.
- Aumentar la difusión de las votaciones que se realicen dentro del Instituto.

## 3. Justificación

El proceso de realizar votaciones ha sido un método de importancia para tomar decisiones en la sociedad, por tal motivo a lo largo de la historia se han utilizado diferentes métodos, ya sea los convencionales con boletas y urnas, incluso otros más directos como correos electrónicos, boletas digitales encriptadas, dispositivos de votación, usando sistemas biométricos o incluso sistemas de votación electrónicos más innovadores. Todos estos métodos mencionados anteriormente han sido de gran ayuda y han dado los resultados esperados, sin embargo, ante la sociedad generan cierta incertidumbre por la manipulación del número de votantes, es decir se podrían suplantar votos adicionales u obtener resultados inexactos, con todo esto es necesario llevar un conteo exhaustivo para generar la confianza que estos sistemas deben de tener.

La conducta ciudadana, que decide en no votar, es frecuentemente descalificada, criticada e incluso objeto de medidas correctivas. A pesar de la imposición gradual del voto universal, de la libre participación de los ciudadanos y de la transparencia de los procesos electorales, es posible afirmar que el avance de los sistemas democráticos no es proporcional al grado de participación el día de los comicios (Nohlen, 2004).

De acuerdo con un artículo consultado de la Revista Mexicana de Sociología [16].

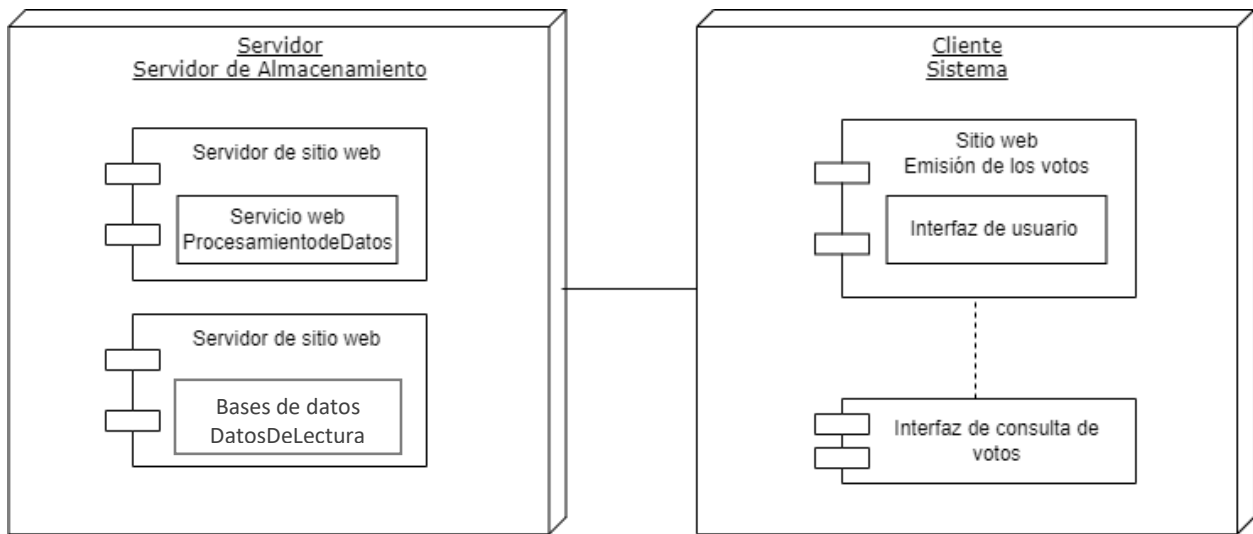
Hoy en día el uso de la tecnología ha sido indispensable en la educación de los jóvenes y más si nos referimos a la comunidad del Instituto Politécnico Nacional, pues el tener acceso a una computadora o un celular es de vital importancia, aunado a la publicación del INEGI sobre la (ENDUTIH) Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares [17], en donde se estimó que en 2020 había 84.1 millones de usuarios de internet en México, que representan 72.0% de la población de seis años o más y que el 91.8% de los usuarios de teléfono celular tiene un equipo inteligente (Smartphone). Es decir, la mayoría de la población cuenta con un teléfono celular y con acceso a internet. Se prevé que este porcentaje año tras año siga aumentando, es por ello que decidimos que el sistema esté disponible para Dispositivos móviles y también para computadoras, así mismo esperamos poder eliminar en gran medida la abstención que se genera en los estudiantes, directivos y PAAE para no votar por cuestiones circunstanciales.

Finalmente creemos que nuestro sistema será desarrollado de tal manera que en un futuro pueda utilizarse para diferentes organizaciones, resolviendo en gran medida la falta de interés y la inseguridad cuando de expresar la opinión democrática se trata, así como también evitar riesgos en la salud y gastos excesivos tomando en cuenta las situaciones que ha padecido la sociedad en estos últimos años.

#### 4. Productos o Resultados esperados

Como resultado del proyecto se pretende obtener los siguientes resultados.

- a. Diseño de la DApp.
- b. Documentación técnica del sistema.
- c. Lanzamiento de Smart Contracts del proyecto.
- d. Lanzamiento de la Página Web.



**Figura 2.** Diagrama a bloques del sistema [Elaboración propia].

## 5. Metodología

La metodología que implementaremos para el desarrollo de nuestro sistema será Espiral, pues con ella, minimizaría los riesgos que conlleva el desarrollo del software, también es muy recomendada para proyectos grandes, el ciclo está representado por las espirales, que se pueden repetir hasta que se entregue la última versión del proyecto y en cada una de las iteraciones, el proyecto va recibiendo mejoras [18].

- Planificación.

Definición de objetivos y alternativas y descripción de las condiciones generales, donde también se estiman costes, programación de actividades y todos los recursos con los que se debe trabajar

- Análisis de riesgo.

Se evalúan e identifican los riesgos que conlleva, y con ello, las soluciones a tales riesgos

- Implementación.

Se lleva a cabo el desarrollo del proyecto donde se incluye la codificación y pruebas, se evalúan los prototipos en un entorno productivo.

- Evaluación del cliente.

En esta parte si hay algunos errores se busca soluciones y si son corregidos se integran al siguiente ciclo.

A continuación, en la figura se anexa un diagrama de la metodología a utilizar



**Figura 2.** Diagrama en espiral [18].

## 6. Cronograma

**Nombre del alumno:** Gutiérrez De La Luz Carlos

**Título del TT:** Propuesta de diseño de una DApp de Votación Digital para la comunidad del Instituto Politécnico Nacional utilizando Blockchain y Smart Contracts.

[illegible]

**Nombre del alumno:** Hernández Tesillos Irving Rodrigo

**Título del TT:** Propuesta de diseño de una DApp de Votación Digital para la comunidad del Instituto Politécnico Nacional utilizando Blockchain y Smart Contracts.

[illegible]



**Nombre del alumno:** Ramírez Arellano Erick Eduardo

**Título del TT:** Propuesta de diseño de una DApp de Votación Digital para la comunidad del Instituto Politécnico Nacional utilizando Blockchain y Smart Contracts.

[illegible]

## 7. Referencias

- [1] N. A. Molano. "Claves para entender la tecnología 'blockchain'". [online] BBVA NOTICIAS. <https://www.bbva.com/es/claves-para-entender-la-tecnologia-blockchain/> (accedido el 12 de abril de 2022).
- [2] X. Moreno Navarro, "Blockchain y su aplicación a los smart contracts", BachelorThesis, Universidad Autónoma de Barcelona, 2019.
- [3] J. Feliu Rey, "Smart Contracts", Tesis, Universidad Carlos III de Madrid, 2018.
- [4] M. Suárez Taboada, "Desarrollo de una aplicación descentralizada con Blockchain: Dapp para el acceso y modificación de información sensible", Trabajo final de Máster, Sistemas Distribuidos, Universitat Oberta de Catalunya, 2020.
- [5] RAE, "votación" Fecha de consulta: 17/04/2022 [Online]. Available: <https://dle.rae.es/votación>
- [6] RAE, "votar" Fecha de consulta: 17/04/2022 [Online]. Available: <https://dle.rae.es/votar>
- [7] RAE, "digital" Fecha de consulta: 17/04/2022 [Online]. Available: <https://dle.rae.es/digital>
- [8] MOE, "Vota Fácil" Fecha de consulta: 17/04/2022 [Online]. Available: <https://www.votafacil.org>
- [9] SaberVotar, "#PiensaTuVoto" Fecha de consulta: 18/04/2022 [Online]. Available: <https://sabervotar.mx>
- [10] INE, "Voto desde el extranjero" Fecha de consulta: 18/04/2022 [Online]. Available: <https://votoextranjero.mx/web/vmre/inicio>
- [11] UCV, "GOOGLE FORMS" Fecha de consulta: 18/04/2022 [Online]. Available: [https://recursostic.ucv.cl/wordpress/index.php/essential\\_grid/formulario-de-google-perfil-estudiante/#1468251697167-ca1eb94c-3fb0](https://recursostic.ucv.cl/wordpress/index.php/essential_grid/formulario-de-google-perfil-estudiante/#1468251697167-ca1eb94c-3fb0)
- [12] Appsamblea - Votaciones online seguras, rápidas y fáciles. (s. f.). Appsamblea - Votaciones online seguras, rápidas y fáciles. <https://appsamblea.com>
- [13] demoKratian, "DEMOKRATIAN" Fecha de consulta: 18/04/2022 [Online]. Available: <https://www.demokratian.org>
- [14] R. Quintana, "Sistema de votación electrónica con autenticación biométrica para ESCOM", Tesis de Grado, Instituto Politécnico Nacional, Escuela Superior de Cómputo, México, 2015.
- [15] SIVE, "Sistema Institucional de Votación Electrónica (SIVE)" Fecha de consulta: 28/04/2022 [Online]. Available: <https://sive.ipn.mx>
- [16] B. Lutz, "La participación electoral inconclusa: abstencionismo y votación nula en México", *Revista mexicana de sociología*, vol. 67, n.º 4, 2005.[En línea]. Disponible: [http://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S0188-25032005000400005](http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-25032005000400005)
- [17] INEGI, "ENDUTIH", Mexico, Comunicado de prensa Num. 352/21, junio de 2021.[En línea]. Disponible: [https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH\\_2020.pdf](https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf)
- [18] Flórez Hernández, H. A. (2009, 15 de mayo). *Vista de PROCESOS DE INGENIERÍA DE SOFTWARE*. Sistema de revistas científicas Centro de Investigaciones y Desarrollo Científico. <https://revistas.udistrital.edu.co/index.php/vinculos/article/view/4141/5806>

## 8. Alumnos y Directores

*Gutiérrez de La luz Carlos.* - Alumno de la  
carrera de Ing. en Sistemas Computacionales en ESCOM,  
Especialidad en Sistemas, Boleta: 2019630244  
Tel. 5562014593 email cgutierrezd1500@alumno.ipn.mx

Firma: \_\_\_\_\_



*Hernandez Tesillos Irving Rodrigo.* - Alumno de la  
carrera de Ing. en Sistemas Computacionales en ESCOM,  
Especialidad en Sistemas, Boleta: 2019630204,  
Tel. 5545476654, email ihernandezt1502@alumno.ipn.mx

Firma: \_\_\_\_\_



*Ramírez Arellano Erick Eduardo.* - Alumno de la  
carrera de Ing. en Sistemas Computacionales en ESCOM,  
Especialidad en Sistemas, Boleta: ,  
Tel. 5572231603, email eramireza1500@alumno.ipn.mx

Firma: \_\_\_\_\_



*Erick Eugenio Linares Vallejo.* - Ingeniero en  
comunicaciones y electrónica (2004), maestría  
en ciencias en electrónica (2010), doctorado  
en ingeniería electrónica y eléctrica (2018),  
Áreas de Interés: Electrónica digital, electrónica,  
sistemas fotónica, sistemas automotrices, email: elinares@ipn.mx

Firma: \_\_\_\_\_



CARÁCTER: Confidencial  
FUNDAMENTO LEGAL: Artículo 11 Fracc. V y Artículos  
108, 113 y 117 de la Ley Federal de Transparencia y Acceso  
a la Información Pública.  
PARTES CONFIDENCIALES: Número de boleta y teléfono.