SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO BLOCKCHAIN

DANIEL ESTEBAN BARRETO AVILA
JULIAN ESTEBAN VALLEJO GALINDO

UNIVERSIDAD DE CUNDINAMARCA
Facultad de Ingeniería
Programa de Ingeniería de Sistemas Facatativá

Facatativá, 2020

SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO BLOCKCHAIN

AUTORES
DANIEL ESTEBAN BARRETO AVILA
JULIAN ESTEBAN VALLEJO GALINDO

Director: Cesar Yesid Barahona Rodríguez

GRUPO DE INVESTIGACIÓN DE SISTEMAS Y TECNOLOGÍA DE FACATATIVÁ **(GISTFA)**

UNIVERSIDAD DE CUNDINAMARCA
Facultad de Ingeniería
Programa de Ingeniería de Sistemas Facatativá

Facatativá, 2020

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____

Presidente jurado

_____

Jurado

_____

Jurado

Facatativá, 2020

COMPROMISO DE AUTOR

Yo Daniel Esteban Barreto Avila con la cedula de identidad No.1070973354 y con código 461214204 estudiante del programa de ingeniería de sistemas de la universidad de Cundinamarca, declaro que:

El contenido del presente documento es un reflejo de nuestro trabajo personal y manifiesto que, ante cualquier notificación de plagio, copia o falta a la fuente original, somos responsables directos legal, económico y administrativo sin afectar el director del trabajo, a la universidad y a cuantas instituciones hayan colaborado en dicho trabajo, asumiendo las consecuencias derivadas de tales practicas

Firma: _____

COMPROMISO DE AUTOR

Yo Julian Esteban Vallejo Galindo con la cedula de identidad 1016107675 y con el código 461215257 estudiante del programa de ingeniería de sistemas de la universidad de Cundinamarca, declaro que:

El contenido del presente documento es un reflejo de nuestro trabajo personal y manifiesto que, ante cualquier notificación de plagio, copia o falta a la fuente original, somos responsables directos legal, económico y administrativo sin afectar el director del trabajo, a la universidad y a cuantas instituciones hayan colaborado en dicho trabajo, asumiendo las consecuencias derivadas de tales practicas

Firma: _____

RESUMEN

Este proyecto tiene como finalidad mostrar el funcionamiento, características y aplicaciones de la red Blockchain en una votación por internet.

En la actualidad el sistema electoral colombiano tiende a tener varios déficits, tales como el error humano y la confianza de los usuarios al momento de implementar cualquier votación que permita la participación de la ciudadanía en la toma de decisiones, además se dará a entender cómo funcionan los Smart contracts o más conocidos como contratos inteligentes.

Ahora bien, en la actualidad los Smart contracts y Blockchain es un sistema revolucionario, su estudio permitirá ver la magnitud de lo que puede aportar global y tecnológicamente al servicio de la comunidad. En este caso se diseñó un sistema de voto electrónico para los cuerpos colegiados de la universidad de Cundinamarca siendo está una Dapp que es ciertamente la integración Blockchain con contratos inteligentes.

Palabras claves: Blockchain, Sistema, plataforma web, Smart contracts, Dapp.

ABSTRACT

This project aims to show the operation, characteristics and applications of the Blockchain network in an internet vote.

Currently, the Colombian electoral system tends to have several deficits, such as human error and user confidence when implementing any vote that allows the participation of citizens in decision-making, and it will also be understood how they work. Smart contracts or better known as smart contracts.

Nowadays, Smart contracts and Blockchain is a revolutionary system, its study will allow us to see the magnitude of what it can contribute globally and technologically to the service of the community. In this case, an internet voting web platform was designed for the collegiate bodies of the University of Cundinamarca, being a Dapp that is certainly the Blockchain integration with smart contracts.

Keywords: Blockchain, System, web platform, Smart contracts, Dapp

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

I. INTRODUCCION

Una Blockchain es esencialmente una base de datos distribuida en una cadena de bloques o libro de contabilidad pública de todas las transacciones o eventos digitales que se han ejecutado y compartido entre las partes participantes, cada transacción en ese libro se verifica por conceso de la mayoría de usuarios que son participantes del sistema. Una vez ingresada la información nunca puede ser borrada, la cadena de bloques contiene un registro determinado y verificable de cada transacción realizada (M. crosby, 2016).

Actualmente en Colombia se viene dando un gran debate a la reforma del código electoral, además de que nos enfrentamos a nuevos retos que se presentan por avance tecnológico en el desarrollo de las democracias (Jenny Garzon,2016).

Por consiguiente es fundamental implementar el voto por internet en Colombia y facilitar el desarrollo de las distintas formas de participación ciudadana, lo anterior tiene como consecuencia un cambio administrativo en las entidades estatales y así poder enfrentar esta nueva implementación del voto, debido a la ley 894 del 2004 estableciendo que las autoridades encargadas de las elecciones deben realizar esta implementación con el fin de estar acorde con las tendencias internacionales y mejore la democracia del país.

Por consiguiente, se está desarrollando un sistema de votaciones por internet que contiene tres partes principales: La primera parte el votante tendrá que seguir una serie de pasos para quedar registrado en el sistema ,La segunda parte del sistema abarca todo lo relacionado a la página web donde se realizará la votación y se mostraran los candidatos y sus respectivas graficas; La tercera parte abarca todo lo relacionado a la seguridad de dicho voto en la cual se implementarán Smart Contracts y la tecnología de Blockchain que aseguraran que la información del voto no se vea modificada.

1. INFORME DE INVESTIGACIÓN

1.1. ESTADO DEL ARTE

En la época que actualmente nos encontramos, se han encontrado diversas formas de asegurar el voto electrónico, pero ninguna de ellas ha sido valida ante los ataques cibernéticos que se pueden presentar, así que el voto por la internet se vuelve inseguro, de la misma manera el centro de innovación y tecnología (CIT) ve la necesidad de implementar un software que logre cumplir con los requisitos para que el voto vía internet sea seguro para los cuerpos colegiados de la universidad de Cundinamarca, entre los cuales se encuentran: Consejo Superior Universitario, Consejo Académico y Consejo de Facultad; Se pretende mejorar de forma radical estos procesos de votación para así hacerlos más óptimos y finalmente seguros implementando Blockchain.

Primeramente, la Blockchain se creó para manejar el historial de transacciones del bitinio además de ofrecer una base de datos inmutable dicho de otra manera, una base de datos que no puede ser alterada o modificada, basada en una secuencia de bloques, estos al ser públicos generan una confianza en base a la transparencia y la solidez de la misma, ciertamente todo lo que se encuentra en la red siempre va a tener una brecha de seguridad, es decir que hasta el momento la red Blockchain no ha sido hackeada (Dolader et al., 2017).

Con la Blockchain lo que se busca principalmente es un sistema donde las entidades de control queden en segundo plano y donde las operaciones se puedan realizar de usuario a usuario(Fallis, 2013).

En particular, el campo de sistemas de votación criptográfica sobre Blockchain es sumamente reciente. A pesar de su poco desarrollo la implementación de Blockchain hace que las elecciones sean sumamente seguras(Caamaño & Sabucedo, 2018).

Igualmente, la tecnología Blockchain ofrece una plataforma descentralizada, es decir que permite a los usuarios enviar datos de forma segura, para que el proceso de votación sea totalmente transparente y responsable con los resultados, del mismo modo las personas que participen en esto sabrán que el proceso es totalmente claro, ya que sus votos no serán alterados y su identidad no tendrá ningún riesgo(De, 2008).

Tabla 1: Inicios de la Blockchain y diferencias entre sus implementaciones en India y Estonia

INDIA	ESTONIA
Se inicia votación electrónica en el año 2002	Se realiza el primer intento de voto por internet en el año 2005
Maneja confianza en el nivel de la votación popular	Se creó el sistema más famoso conocido como i-voting
Se usaron las maquinas EVM (electronic voting machine)	No era seguro ya que se usaron entornos no controlados (casa, lugar público)

Los votantes no tenían que ser monitoreados mientras votaban por los auditores	Solo se contaba el último voto
	Los ciudadanos podían votar un día con anterioridad
	Se intentó hackear, pero fue imposible, llegando a votar más del 24% de la población

Fuentes: (Grado,2019), (Del,2014).

Para hacer posible la votación web con implementación de Blockchain se deben trabajar mucho en protocolos remotos de votación electrónica utilizando herramientas criptográficas como por ejemplo (TTP) que está involucrado para hacer que los sistemas de votación electrónica se implementen más fácilmente y revisado(Liu & Wang, 2017).

Actualmente existen sistemas de votación electrónica que se ofrecen como soluciones completas prestadas por empresas privadas. Las cuales son Smartmatic y Scytl son dos de las más relevantes a nivel internacional ubicadas en España(Caamaño & Sabucedo, 2018).

Sin embargo, los sistemas de votación de software libre con uso en casos reales escasean, siendo de especial mención los pocos que reciben el mayor uso: nVotes (anteriormente conocido como Agora Voting), utilizado en las consultas internas del partido político español Podemos; y Helios Voting, desarrollado como un sistema de auditoría abierta, cuyo uso públicamente se limita a elecciones universitarias(Caamaño & Sabucedo, 2018).

Por otro lado, y según Grado, se encuentran diversos tipos de Blockchain, las cuales se explicarán a continuación:

1. Blockchain públicas: Cualquier puede acceder y consultar transacciones realizadas, se permite a los usuarios hacer transacciones a la base de datos, igualmente no se pueden alterar, pero se pueden verificar, son descentralizadas ya como se mencionó anteriormente ningún usuario tiene mayor jerarquía que otro, los usuarios son rastreables debido a que la Blockchain es pública

2. Blockchain privadas: No todos los datos inscritos son públicos y únicamente los usuarios que componen la red privada pueden acceder a esta y asimismo hacer consultas y transacciones, el número de nodos que componen este tipo de red es limitado al número de usuarios, ciertamente este tipo de Blockchain nos asegura el anonimato que es requerido para cualquier realización o protección de transacciones

3. Blockchain hibridas: es la combinación de las públicas y privadas, el tipo de red de está Blockchain casi nunca están abiertas y son gestionadas por varias entidades, se usa por gobiernos y empresas que producen grandes cantidades de transacciones (Grado, 2019).

Tabla 2: Comparación entre la implementación de Blockchain en los países Noruega y Sierra Leona

NORUEGA	SIERRA LEONA (ÁFRICA)
Este país es reconocido por su alto avance en el campo de e-voting implementando Blockchain publicas	Es el primer país del mundo en usar Blockchain
Se pudo votar desde cualquier lugar publico	Participaron 16 candidatos en el que el ganador fue el presidente Ernest Bai
Solo se contaba el último voto debido a que se podía votar más de una vez	
Al ser uno de los países pioneros en el tema de voto electrónico tuvieron fallas de seguridad	La empresa que desarrollo esta tecnología es Agora reduciendo así costos para la votación popular
No era seguro ya que se usaron entornos no controlados (casa, lugar público) y se encontró redundancia de datos	Se usa una Blockchain privada para poder supervisar los resultados en tiempo real
	Está basado en Blockchain publica de Ethereum

Fuente: (Fusco et al., 2018).

Tabla 3*:* Comparativa Tecnologías Blockchain y Web en Estados Unidos y Nueva Gales

ESTADOS UNIDOS	NUEVA GALES (del Sur)
Se propone un protocolo de votación en 2015 implementando Blockchain y contratos inteligentes	Se hace una prueba piloto por medio de una app web en la que votaron 280000 usuarios
Se aplicó un esquema de recompensa/penalización por conductas correctas o incorrectas de los votantes	Se implementa un aplicativo web que requería ciertos pasos para validar el voto
Es el primer intento de combinar la votación electrónica con Blockchain implementando contratos inteligentes	Los pasos constan en un previo registro ante un ente gubernamental, inicio de sesión con un id y un PIN (12 Dígitos) y por último puede verificar si su voto fue incluido
En 2016 se propone un protocolo de votación electrónica, basado en TTP y Blockchain	

Fuente: (Ben Ayed, 2017), (Liu & Wang, 2017).

Ciertamente y no menos importante se encuentra los contratos inteligentes, en los que el país de Suecia ha hecho bastante énfasis debido a que estos son secuencias de código que implementan acuerdos previamente ya existentes, de la misma manera se puede producir aspectos a nivel jurídico, la principal característica es que se ejecutan de manera autónoma, estos usan la tecnología de bloques Blockchain ya mencionada anteriormente.

Agregando a lo anterior una de las ventajas es que los scripts de estos son sumamente susceptibles, esto se puede se convertir en una tarea simple como

por ejemplo el simple hecho de ejecutar un voto o algo más complejo como ejecutar un pago de cualquier servicio, estos contratos son sencillos, rápidos e inmodificables(SÁENZ, 2017).

Tabla 4: Comparativa de lo que se ha implementado en Colombia y en Suecia respecto a tecnologías Blockchain implementadas en voto electrónico

COLOMBIA	**SUECIA**
Se aplican varias propuestas legislativas en las cuales se busca sacar el máximo provecho de las tecnologías Blockchain	Se desarrollan sistemas de Contratos Inteligentes y tecnología Blockchain orientados a votaciones de empresas privadas
Se realiza el primer hackathon sobre el tema en Colombia, basándose en el impacto y el futuro del Blockchain con contratos inteligentes	La empresa Telia desarrolla el primer sistema de registro a la propiedad implementando Blockchain y contratos inteligentes implementando así Blockchain hibridas
	Se minimizan los riesgos de pérdida o alteración de la información drásticamente y se agilizan las transacciones

Fuente: (De, 2008), (Bartolomé Pina et al., 2017).

Además de agilizar y mejorar la seguridad en transacciones los contratos inteligentes se guardarán en la red pública de la Blockchain para que no se puedan cambiar las condiciones y de igual manera no se modifiquen sus funciones, la red Ethereum ofrece a los desarrolladores programar agentes autónomos, esto quiere decir dentro del ambiente de ejecución de la misma, a continuación de acuerdo al autor Sergio Martínez Medina (2008), se nombran las características que debe cumplir un contrato inteligente para que este pueda ser plenamente desarrollado:

1. Autonomía: Es donde cada una de las partes hacen acuerdos sin necesidad de ningún tercero, y se evita la manipulación de datos por parte de un tercero
2. Copia de seguridad: la información se guarda en cada nodo de la red y esto hace imposible la perdida de estos datos
3. Velocidad: se pueden recuperar muchas horas de trabajo que anteriormente se gastaban con papeleo
4. Ahorro: evita intermediarios y esto a su vez disminuye los costos
5. Exactitud: se encuentra contratos rápidos, baratos y así mismo se puede garantizar la excelencia de estos (Grado, 2019).

En la actualidad según el Autor (Cavero, 2014) hay varios framework que se encuentran desarrollando contratos inteligentes como por ejemplo Ethereum que permite a otros desarrolladores la creación de aplicaciones descentralizadas como los Smart contracts o contratos inteligentes, a la vez sirve como la plataforma donde se ejecutan estos, este framework aprovecha el mecanismo proof-of-work para la creación de los nuevos bloques en la red Blockchain, se debe tener en cuenta que este protocolo no demorara en cambiar a proof-of-stake con esté el nuevo bloque es elegido de manera aleatoria.

Por consiguiente, se necesita la Ethereum virtual machine (VMC) la cual tiene como misión es facilitar la creación de cualquier aplicación que esté usando Blockchain y así mismo sirve como plataforma segura (Cavero, 2014).

Además, de acuerdo al autor Víctor palacios (2014), se encuentran varios entornos de trabajo como:

1. Remix: Es un entorno de desarrollo online basado en un navegador con entorno de pruebas, se puede instalar en máquinas localmente o usar el navegador favorito

2. Ganache: Es una cadena de bloques personal para el desarrollo de DApps Ethereum que puede utilizar para implementar contratos, desarrollar sus aplicaciones y ejecutar pruebas

3. Truffle Suite**:** Es un entorno de desarrollo que facilita la integración de contratos inteligente en la cadena de bloques, convirtiendo lenguaje de programación como solidity a binario que es el formato que acepta la Blockchain

4. Solidity**:** Es un lenguaje de programación de alto nivel creado en el 2014 para aumentar el acceso a este tipo de tecnología, está basado en JavaScript lo cual nos permite crear contratos inteligentes de una forma más amigable con el programador

5. Web3.js: Es una librería que permite interactuar con nodos de Ethereum locales o remotos utilizando conexión http, WebSocket o IPC

6. MetaMask**:** Un puente que le permite visitar la red Blockchain en su navegador hoy le permite ejecutar Ethereum DApps directamente en su navegador sin ejecutar un nodo completo de Ethereum(Cavero, 2014).

En el mercado se encuentran las DApps estas son las aplicaciones que usan un contrato inteligente en una red de Blockchain (Decentralized application) , para poder crear una red en Ethereum esté es el software que se va a implementar para poder es necesario contar con la dirección del Blockchain o el más conocido (wallet) , la cual permite realizar transacciones dentro de la Blockchain, después de esto se puede crear el nodo dentro para asociarlo al wallet anterior, como muestra de la unión del wallet y el nodo quedara el (Smart contract) , que define los requerimientos que implemente el aplicativo (Goyena, 2019).

Resumiendo, la tecnología Blockchain y los contratos inteligentes, pueden reducir los tiempos necesarios para completar transacciones y mejoran la seguridad de procesos lo cual se evidencia al hacer las comparativas entre países europeos, africanos, asiáticos y americanos y los resultados obtenidos son una clara evidencia del potencial que ofrece la Blockchain combinados con Ethereum.

1.2. LINEA DE INVESTIGACIÓN

La plataforma web de votaciones se desarrollará bajo la línea de **investigación software sistemas emergentes y nuevas tecnologías.**

Esta línea de investigación se encarga de solucionar problemas en la universidad de Cundinamarca extensión Facatativá, Esto se sitúa en el campo de la innovación y desarrollo de software. La Blockchain como implementación de seguridad y confianza manejando distintas herramientas para el desarrollo como el uso de una cadena de bloques local para encriptar las transacciones dentro del sistema, Sistemas emergentes como aplicaciones de forma descentralizada y aplicando contratos inteligentes lo cual nos lleva a automatizar el proceso y eliminar intermediarios.

El software plantea la sistematización del voto para los cuerpos colegiados de la universidad de Cundinamarca lo cual nos facilita el conteo de votos de los sufragantes y haciendo un proceso más fácil y accesible para los estudiantes.

Posteriormente a esto, el centro de investigación y tecnología (CIT) ve la necesidad de implementar un software mediante un sistema unificado, que logre cumplir con los requisitos para que el voto vía internet sea seguro para los cuerpos colegiados de la universidad de Cundinamarca, el cual tendrá todas las herramientas sistemáticas para generar la suficiente confianza de un voto popular.

En este orden de ideas la tecnología Blockchain ofrece una plataforma descentralizada, es decir, envía datos de forma segura, para que el proceso de votación sea totalmente transparente y responsable con los resultados, del mismo modo las personas que participen en esto sabrán que el proceso es totalmente claro, ya que sus votos no serán alterados y su identidad no tendrá ningún riesgo

1.3. PLANTEAMIENTO DEL PROBLEMA Y PREGUNTA DE INVESTIGACIÓN

El principal inconveniente en los sistemas de votación es la centralización que genera que los usuarios no tengan la suficiente confianza para usar estos sistemas, es por eso que el uso de las tecnológicas libres es la clave en el desarrollo del proyecto, estos sistemas se basan en la confianza y desafortunadamente en Colombia la cultura alrededor de la política y sus procesos es de desconfianza y es algo que se debe dejar a un lado y así mismo hacer uso de software libre(Dolader et al., 2017).
Además, se estudia actualmente la implementación del voto electrónico en el sistema electoral colombiano, el gran reto de la introducción de tecnologías de información al sistema electoral tendrá que ver, necesariamente, con garantizar la transparencia de las elecciones y la generación de confianza en el ciudadano y en los candidatos, sobre todo en los resultados (Del, 2014).

Actualmente en la Universidad de Cundinamarca el sistema de votación para la elección de representantes se lleva a cabo por medio de cartones y votos físicos en hojas de papel por lo que la información de los votos puede ser alterada, lo que genera que el voto sea menos seguro y pueda ser modificado

debido a que este sistema cuenta con un problema y es la centralización y manipulación del proceso y la información de los votos, lo que significa que una persona o entidad es encargada de controlar el sistema, la base de datos o información de cada voto, disminuyendo así la seguridad de cada voto y su información.

Siendo evidenciada está problemática en nuestro entorno, se origina el siguiente interrogante:

¿Cómo implementar la tecnología Blockchain en el proceso de votación de cuerpos colegiados en la Universidad de Cundinamarca?

1.4. OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS

Objetivo General

Desarrollar e implementar el módulo de la red Blockchain para el sistema de voto electrónico para los Cuerpos Colegiados de la universidad de Cundinamarca**.**

Objetivos Específicos

- Plantear requerimientos basados en estudios realizados a la red Blockchain
- Diseño de contrato inteligente para realizar una votación
- Realizar el modelado pertinente para llevar a cabo el desarrollo de la red Blockchain
- Desarrollo de la red Blockchain implementando contrato inteligente
- Analizar resultados obtenidos en el escenario de pruebas de la red Blockchain
- Integrar el módulo blockchain a el sistema de voto electrónico para los cuerpos colegiados de la universidad de Cundinamarca.
- Analizar impacto social del proyecto utilizando metodología de investigación mixta NVivo
- Realizar prueba SonarQube

1.5. ALCANCE E IMPACTO DEL PROYECTO

La universidad de Cundinamarca tiene como fin principal trasmitir conocimiento, así mismo su objetivo es formar para la vida, los valores democráticos, la civilidad y la libertad, con el fin de trascender al departamento, la nación, y el mundo, por consiguiente es de vital importancia la formación de profesionales competentes que contribuyan con sus habilidades y capacidades a la realización de una mejor sociedad, ahora bien, está debe caracterizarse por ser una organización en un constante proceso de renovación, que opera en tiempo real y donde los servicios administrativos y no administrativos sean prestados en línea, a través de plataformas o aplicaciones tecnológicas que reduzcan los tiempos de respuesta ante solicitudes de cualquier naturaleza(*PLAN ESTRATÉGICO 2016 - 2026*, 2016).

Posteriormente a esto, el centro de investigación y tecnología (CIT) ve la necesidad de implementar un software mediante un sistema unificado, que logre

cumplir con los requisitos para que el voto vía internet sea seguro para los cuerpos colegiados de la universidad de Cundinamarca, el cual tendrá todas las herramientas sistemáticas para generar la suficiente confianza de un voto popular.

La Organización de las Naciones Unidas (ONU) tiene 16 objetivos de desarrollo sostenible, ahora bien, puede ser entendido de manera global como el mantenimiento o el mejoramiento de las “condiciones de calidad” del sistema de interrelaciones sociedad-naturaleza. El propósito de estos ODS es crear un conjunto de objetivos mundiales relacionados con desafíos ambientales, económicos y políticos que afectan nuestro entorno. El desarrollo de este tipo de sistemas contribuye a objetivos en este caso nos enfocaremos en el número 16 debido a que este ODS busca hacer frente a desafíos de inseguridad y construir sociedades más pacíficas e inclusivas, por lo que es necesario que se establezcan reglamentaciones más eficientes y transparentes, y presupuestos gubernamentales integrales y realistas haciendo uso de una óptima y eficiente utilización de medios tecnológicos para combatir la corrupción, el soborno y el robo, para así reducir considerablemente la corrupción y el soborno en todas sus formas.

En ese proceso participan distintos interesados, entre ellos empresas, universidades, consumidores, encargados de la formulación de políticas, investigadores, científicos, minoristas, medios de comunicación y organismos de cooperación para el desarrollo.

Además de lo anterior se debe implementar el voto por internet en Colombia y facilitar el desarrollo de las distintas formas de participación ciudadana, lo anterior tiene como consecuencia un cambio administrativo en las entidades estatales y así poder enfrentar esta nueva implementación del voto, lo anterior debido a la ley 894 del 2004 estableciendo que las autoridades encargadas de las elecciones deben realizar esta implementación con el fin de estar acorde con las tendencias internacionales y mejore la democracia del país, actualmente en Colombia se viene dando este gran debate a la reforma del código electoral colombiano, además de que nos enfrentamos a nuevos retos que se presentan por avance tecnológico en el desarrollo de las democracias (Jenny Garzon,2016).

En este orden de ideas la tecnología Blockchain ofrece una plataforma descentralizada, es decir, envía datos de forma segura, para que el proceso de votación sea totalmente transparente y responsable con los resultados, del mismo modo las personas que participen en esto sabrán que el proceso es totalmente claro, ya que sus votos no serán alterados y su identidad no tendrá ningún riesgo(De, 2008).

Con la red Blockchain lo que se busca principalmente es un sistema donde las entidades de control queden en segundo plano y donde las operaciones se puedan realizar de usuario a usuario(Fallis, 2013).

1.6. METODOLOGÍA

METODOLOGÍA DE INVESTIGACIÓN Y DESARROLLO

La universidad de Cundinamarca tiene como fin principal trasmitir conocimiento, así mismo su objetivo es formar para la vida, los valores democráticos, la civilidad y la libertad, con el fin de trascender al departamento, la nación, y el mundo, por consiguiente es de vital importancia la formación de profesionales competentes que contribuyan con sus habilidades y capacidades a la realización de una mejor sociedad, ahora bien, está debe caracterizarse por ser una organización en un constante proceso de renovación, que opera en tiempo real y donde los servicios administrativos y no administrativos sean prestados en línea, a través de plataformas o aplicaciones tecnológicas que reduzcan los tiempos de respuesta ante solicitudes de cualquier naturaleza(*PLAN ESTRATÉGICO 2016 - 2026*, 2016).

Posteriormente a esto, el centro de investigación y tecnología (CIT) ve la necesidad de implementar un software mediante un sistema unificado, que logre cumplir con los requisitos para que el voto vía internet sea seguro para los cuerpos colegiados de la universidad de Cundinamarca, el cual tendrá todas las herramientas sistemáticas para generar la suficiente confianza de un voto popular.

La Organización de las Naciones Unidas (ONU) tiene 16 objetivos de desarrollo sostenible, ahora bien, puede ser entendido de manera global como el mantenimiento o el mejoramiento de las “condiciones de calidad” del sistema de interrelaciones sociedad-naturaleza. El propósito de estos ODS es crear un conjunto de objetivos mundiales relacionados con desafíos ambientales, económicos y políticos que afectan nuestro entorno. El desarrollo de este tipo de sistemas contribuye a objetivos en este caso nos enfocaremos en el número 16 debido a que este ODS busca hacer frente a desafíos de inseguridad y construir sociedades más pacíficas e inclusivas, por lo que es necesario que se establezcan reglamentaciones más eficientes y transparentes, y presupuestos gubernamentales integrales y realistas haciendo uso de una óptima y eficiente utilización de medios tecnológicos para combatir la corrupción, el soborno y el robo, para así reducir considerablemente la corrupción y el soborno en todas sus formas.

En ese proceso participan distintos interesados, entre ellos empresas, universidades, consumidores, encargados de la formulación de políticas, investigadores, científicos, minoristas, medios de comunicación y organismos de cooperación para el desarrollo

Además de lo anterior se debe implementar el voto por internet en Colombia y facilitar el desarrollo de las distintas formas de participación ciudadana, lo anterior tiene como consecuencia un cambio administrativo en las entidades estatales y así poder enfrentar está nueva implementación del voto, lo anterior debido a la ley 894 del 2004 estableciendo que las autoridades encargadas de las elecciones deben realizar esta implementación con el fin de estar acorde con las tendencias internacionales y mejore la democracia del país, actualmente en Colombia se viene dando este gran debate a la reforma del código electoral colombiano, además de que nos enfrentamos a nuevos retos que se presentan

por avance tecnológico en el desarrollo de las democracias (Jenny Garzon,2016).

En este orden de ideas la tecnología Blockchain ofrece una plataforma descentralizada, es decir, envía datos de forma segura, para que el proceso de votación sea totalmente transparente y responsable con los resultados, del mismo modo las personas que participen en esto sabrán que el proceso es totalmente claro, ya que sus votos no serán alterados y su identidad no tendrá ningún riesgo(De, 2008).

Con la red Blockchain lo que se busca principalmente es un sistema donde las entidades de control queden en segundo plano y donde las operaciones se puedan realizar de usuario a usuario(Fallis, 2013).

1.7. MARCOS DE REFERENCIA

1.7.1. MARCO TEÓRICO

Para la democracia en distintos países y lugares del mundo los sistemas de votación son indispensables, su principal objetivo es la elección de representantes, presidentes, líderes de comunidades siendo el sector político quien ha tenido a lo largo de la historia mayor influencia. El voto electrónico se ha implementado en distintas elecciones para facilitar el conteo de sufragios, menos complicaciones al momento del voto y mayor seguridad, aunque esta última no se cumple del todo ya que se considera el voto electrónico como vulnerable o propenso a manipulación porque muchos entes del gobierno y otros sectores pueden tener acceso a varios niveles del sistema.

“La democracia electrónica, a través del voto electrónico, brinda la posibilidad a los ciudadanos de participar permanentemente en las decisiones políticas. Esta modalidad participativa surge en los años 60, cuando los investigadores empezaron a descubrir el potencial cívico de la nueva tecnología electrónica. Adquiere mayor relevancia con la evolución tecnológica y la reducción de la brecha digital, incorporándose masivamente en el ámbito cotidiano de las personas”(Pesado et al., 2008).

Una Blockchain es una base de datos descentralizada donde su uso principalmente para la transferencia de criptomonedas pero un tiempo después se vio el potencial que tenía esta tecnología y varias formas nuevas para su implementación, Dado la seguridad y confianza que genera una Blockchain al ser un sistema con duplicidad de información y sin un dueño en concreto debido a su descentralización donde diferentes partes tienen que aprobar sus transacciones para luego ser almacenadas en su cadena de bloques aquí nacieron los contratos inteligentes.

“La cadena de bloques es una secuencia de bloques, que contiene una lista completa de registros de transacciones como el libro público convencional (Lee Kuo Chuen, 2015). Cada bloque apunta al bloque

anterior a través de una referencia que es esencialmente un valor hash del bloque anterior llamado bloque de padres. Cabe resaltar que los hashes de bloques de tío (hijos de los antepasados del bloque) también se almacenarían en ethereum blockchain (Buterin, 2014). El primer bloque de una cadena de bloques se llama bloque de génesis, que no tiene bloque primario.” (Wang et al., 2018).

Para la cadena de bloques es indispensable contar con puntos de transacciones que descentralicen la red como lo son los nodos. Todos los registros o transacciones que se contienen en la Blockchain son duplicados en los diferentes nodos que componen la red manteniendo una copia completa y actualizada de la cadena que se está formando, estos tienen la función de generar nuevos bloques y hacer una validación de los que se van a añadir a la cadena, como cada bloque va cifrado en un código hash lo que hacen estos es buscar ese código para así poder generar otro basado en el hash anterior y los demás nodos verifican si el hash seleccionado para el nuevo bloque es correcto basado en los anteriores. De esta forma se está haciendo un sistema de consenso donde para dar como aprobado un bloque se necesita que al menos el 51% de nodos en la cadena existente hayan validado con éxito el bloque. Estos nodos son bien llamados mineros quienes son los que se encargan de poner su máquina para estos procesos ya que consume bastantes recursos de hardware para poder procesar estos hashes, por lo tanto, ellos son recompensados por el nivel de transacciones validadas o procesadas en alguna criptomoneda dependiendo la red en la que se encuentren minando.

Las Blockchain pueden clasificarse en tres tipos públicas, privadas o hibridas:

1. Blockchain públicas: Cualquier puede acceder y consultar transacciones realizadas, se permite a los usuarios hacer transacciones a la base de datos, igualmente no se pueden alterar, pero se pueden verificar, son descentralizadas ya como se mencionó anteriormente ningún usuario tiene mayor jerarquía que otro, los usuarios son rastreables debido a que la Blockchain es pública
2. Blockchain privadas: No todos los datos inscritos son públicos y únicamente los usuarios que componen la red privada pueden acceder a esta y asimismo hacer consultas y transacciones, el número de nodos que componen este tipo de red es limitado al número de usuarios, ciertamente este tipo de Blockchain nos asegura el anonimato que es requerido para cualquier realización o protección de transacciones
3. Blockchain hibridas: es la combinación de las públicas y privadas, el tipo de red de está Blockchain casi nunca están abiertas y son gestionadas por varias entidades, se usa por gobiernos y empresas que producen grandes cantidades de transacciones (Grado, 2019).

En la cadena hay un bloque que predomina sobre los demás ya que no tiene ningún antecesor a este se le llama bloque Génesis, es el más importante porque es donde va configurado el funcionamiento de la

Blockchain. Este bloque es el que da una identidad sobre toda la cadena es decir dos nodos no se pueden comunicar si no pertenecen al mismo bloque génesis ya que los códigos hash serian diferentes y por lo tanto estos nodos no serían compatibles.

Un contrato inteligente es una forma codificada de un contrato de papel donde se ponen unas pautas o condiciones por cumplir entre dos partes para intercambiar un bien o servicio teniendo un intermediario en este caso alguien de índole jurídico que haga valer este contrato, donde este contrato se ejecuta automáticamente después de llegar a un acuerdo entre los involucrados se escriben en código de computadora las condiciones y este retiene el valor a intercambiar hasta que no se cumpla dicho contrato cabe aclarar que después de ejecutar el contrato este no se puede modificar hasta su finalización.

Al ser un contrato automatizado es decir que se ejecuta por su propia cuenta se eliminan dichos intermediarios haciendo del proceso algo más confiable y más económico, estos contratos se insertan en la Blockchain para que estos se puedan ejecutar de forma satisfactoria evitando una manipulación de los datos de cada transacción.

1.7.2. MARCO LEGAL

La plataforma web es un sistema descentralizado que no tiene uso de terceros para que así las votaciones por la misma sean transparentes, de esta forma se dará uso al derecho del voto de los estudiantes. Teniendo en cuenta la legislación que tiene la universidad ante el sistema electoral de los cuerpos colegiados.

Blockchain, como tecnología, no se puede regular: solo se pueden regular las actividades que la utilizan. Sin embargo, existen retos regulatorios transversales que, independientemente del caso de uso específico, van a estar presentes y que tendrán que abordarse para facilitar su adopción (Alvaro marin,2017).

De acuerdo con el marco legal colombiano vigente, *Bitcoin*, las monedas digitales y Blockchain son vistas como un bien mueble, por lo cual las actividades comerciales para su compra venta plantearía el requerimiento de licencias, lo cual podría dar pie a muchas controversias ya que de momento **no hay una posición jurídica en relación a cómo actuar hacia ella desde lo tributario.** Sin embargo, se ha dejado muy claro desde las posiciones oficiales de los representantes de las instituciones gubernamentales que *Bitcoin* o Blockchain no puede ser equivalente en ninguna medida a la moneda de circulación nacional (Erick rincón,2017).

Rincón aseguró que el estado ha comenzado desde hace años a dar pasos importantes en cuanto a fijar una postura hacia las monedas digitales, ya que el Banco de la República emitió un documento sobre los beneficios de la regulación para las criptomonedas.

En Colombia existen algunas leyes (527, artículo 17) y circulares (029, 052 y 042) que avalan de alguna manera el uso de las nuevas tecnologías en los procesos comerciales.

La incorporación del voto electrónico en Colombia se promulgo en la ley 892 de 2004 y se reiteró con el artículo 39 de la ley 1475 del 2011 pero no se ha implementado debido a sus costos en hardware y software que habría que hacer para su primera implementación.

II. DOCUMENTACIÓN DE SOFTWARE

2.1. PLAN DE PROYECTO

de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
	Fase de aprendizaje	**52 días**	**mar 10/03/2**	**mié 20/05/20**		
	Desplegar blockchain	9 días	mar 10/03/20	vie 20/03/20		Daniel Barreto
	aprender lenguaje solidity	11 días	lun 23/03/20	lun 06/04/20	2	Esteban Vallejo
	programar blockchain publica	11 días	mar 10/03/20	mar 24/03/20		Daniel Barreto- Esteban Vallejo
	instalacion y modificacion ganache	13 días	mié 25/03/20	vie 10/04/20	4	Esteban Vallejo
	uso de cuentas metamask	9 días	lun 13/04/20	jue 23/04/20	5	Daniel Barreto

Figura 1. Plan proyecto (Fase de aprendizaje).

de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
	fase de modelados	**3 días**	**jue 30/04/20**	**sáb 02/05/20**	**6**	
	modelados UML	2 días	mar 10/03/2	mié 11/03/20		Esteban Vallejo
	modelados blockchain	1 día	mar 17/03/20	mar 17/03/20		Daniel Barreto
	desarrollo de la aplicación	**34 días**	**mar 10/03/20**	**vie 24/04/20**		**Daniel Barreto- Esteban Vallejo**
	Smart contract	8 días	mié 18/03/2	vie 27/03/20	9	Daniel Barreto
	Conexión a ganache	8 días	lun 30/03/20	mié 08/04/20	11	Esteban Vallejo
	conexión a metamask	5 días	jue 09/04/20	mié 15/04/20	12	Daniel Barreto
	modulo administrador del smart contract	15 días	jue 16/04/20	mié 06/05/20	13	Daniel Barreto- Esteban Vallejo

Figura 2. Plan proyecto (Fase de modelados y desarrollo de la aplicación)

Fase de pruebas	**80 días**	**lun 03/08/20**	**vie 20/11/20**	**14**	**Daniel Barreto- Esteban Vallejo**
prueba de carga y estrés	50 días	mar 24/03/20	lun 01/06/20	14	Daniel Barreto
analisis de resultados	30 días	vie 25/09/20	jue 05/11/20		Esteban Vallejo

Figura 3. Plan proyecto (Fase de pruebas)

2.2. DETERMINACIÓN DE REQUERIMIENTOS

2.2.1 Introducción

Este documento es una especificación de requisitos de software (ERS) para el sistema de voto electrónico para los Cuerpos Colegiados de la universidad de Cundinamarca, basándose en las directrices estándar IEEE practica recomendada para requisitos específicos de software ANSI/IEEE 830,1998.

El software unificado consta de tres módulos: Módulo blockchain, Módulo front-end y Módulo autenticación, los cuales deben comunicarse para así conformar un sistema seguro y fiable al momento de hacer la votación.

2.2.2. Propósito

El propósito de este documento es informar en la Universidad de Cundinamarca Extensión Facatativá al Programa Ingeniería de Sistemas, los requerimientos de software, del mismo modo definir las especificaciones funcionales y no funcionales, para así hacer optimo el desarrollo de la aplicación para el sistema de voto electrónico de los cuerpos colegiados de la universidad de Cundinamarca (Módulo blockchain).

2.2.3. Ámbito del sistema

El aplicativo web se enfocará en un sistema descentralizado, de la misma manera será un sistema web que utilizará la tecnología blockchain garantizando así que el proceso de votación sea totalmente transparente y responsable con los resultados.

2.2.4. Personal Involucrado

Nombre	Cesar Yesid Barahona Rodríguez
Rol	Director de investigación
Categoría profesional	Ingeniero de Telecomunicaciones
Responsabilidad	
Información de contacto	cbarahona@ucundinamarca.edu.co

Nombre	Daniel Esteban Barreto Avila
Rol	Estudiante de pregrado investigador auxiliar
Categoría profesional	Estudiante de ingeniería de sistemas
Responsabilidad	
Información de contacto	danielebarreto@ucundinamarca.edu.co

Nombre	Julian Esteban Vallejo Galindo
Rol	Estudiante de pregrado investigador auxiliar
Categoría profesional	Estudiante de ingeniería de sistemas
Responsabilidad	
Información de contacto	jevallejo@ucundinamarca.edu.co

2.2.5. Definiciones acrónimos y abreviaturas

Nombres	Descripción
DApps	aplicaciones descentralizadas cuyo funcionamiento se basa en una red centralizada con otros interactuando con otros.
ERS	acuerdo entre la parte desarrolladora y la parte cliente, ambas partes establecen los requisitos de la aplicación.
Blockchain	Cadena de bloques cifradas para almacenar información
Ganache	Herramienta donde se puede tener una blockchain local.
Web3	Librería para manejar nodos Ethereum
Solidity	Es un lenguaje de alto nivel orientado a contratos, su sintaxis es similar a la de JavaScript y está enfocado específicamente a la máquina virtual (EVM).
JavaScript	Es un lenguaje de programación interpretado orientado a objetos conservando las buenas prácticas es imperativo débilmente tipado y dinámico.

2.2.6. Referencias

https://developer.mozilla.org/es/docs/Learn/JavaScript/First_steps/Qué_es_JavaScript

https://www.bbva.com/es/que-son-las-dapps-y-por-que-seran-cada-vez-mas-mportantes/

https://criptotario.com/que-es-solidity

2.2.7. Visión general

El documento de requerimientos se dividirá en tres secciones. La primera sección es una introducción al mismo, se expone el propósito de la plataforma a desarrollar, se definen términos importantes para el entendimiento de este y así lograr una mejor comprensión de lo que se planea realizar.

La segunda sección expone una descripción general de lo que será el producto una vez terminado, dará a conocer sus principales funciones y sus principales restricciones para poder hacer uso de la plataforma propuesta. Dara una idea de cómo estará desarrollado el aplicativo.

En la tercera y última sección, se definen los requisitos y funciones del aplicativo web, que características tienen las distintas interfaces de este.

2.3 . DESCRIPCIÓN GENERAL

Una aplicación descentralizada que tiene como referencia el uso de la red blockchain, está permitirá llevar a cabo la votación de los Cuerpos Colegiados de la universidad de Cundinamarca, así mismo será desarrollada en un entorno de pruebas.

2.3.1. Perspectiva del producto

Sera una aplicación centralizada que trabajara en un entorno web para así hacer fácil el acceso al momento de hacer la votación. De la misma manera este aplicativo es uno de los módulos que contempla el sistema de voto electrónico de la universidad de Cundinamarca, los otros módulos son los siguientes:

- Autenticación.
- Front-end.

. Las funciones más relevantes que tiene este subsistema son las siguientes:

- Implementar y poner en funcionamiento los contratos inteligentes.
- Implementar el uso de la red blockchain.
- Implementar el uso de las DApps.

2.3.2. Funcionalidad del producto

Una Dapp usando la tecnología de la red blockchain donde el estudiante podrá ejercer su derecho al voto como si esté fuera una votación popular, como valor agregado generando confianza de la no alteración de los resultados en la votación ya realizada.

2.3.3. Características de los usuarios

Los usuarios deben ser las estudiantes de la universidad de Cundinamarca, otros usuarios que se deben registrar con el correo y a los cuales el administrador debe aprobar y estos pueden ser agentes externos que tengan algún tipo de vínculo con la institución.

2.3.4. Restricciones

- Complemento MetaMask en el navegador
- Lenguajes y tecnologías en uso: HTML, JavaScript, Solidity, Blockchain.
- Muchos recursos computacionales a la hora de cifrar cada bloque por transacción.
- Se recomienda un navegador web con soporte de HTML5, CSS3 y JavaScript para el acceso a la interfaz de usuario web.

2.3.5. Suposiciones y dependencias

- La plataforma web será desarrollada con un estándar establecido, requiriendo la instalación de framework y librerías para la interfaz de usuario.
- Se asume que los requisitos mínimos del computador donde se trabajara son para uno de bajas características de rendimiento.
- Se asume que los requisitos establecidos permanecerán estables.

2.3.6. Requisitos futuros

La aplicación a futuro podrá instalarse para que se pueda votar en cualquier ámbito local, nacional, dando así más soporte y donde no solo se integre a la universidad de Cundinamarca sino también a la persona natural.

2.4. Requisitos Específicos

2.4.1. Interfaces externas

- Un aplicativo web para el sistema de voto electrónico para los Cuerpos Colegiados de la universidad de Cundinamarca.
- Con base en el aspecto de aplicativo web, cada ordenador en donde sea necesario acceder a la página web deberá contar con acceso a internet, esto debido a que es el medio de comunicación con el servidor del aplicativo.
- Este aplicativo podrá usarse en computadores con navegadores web actualizados.
- Navegador web con soporte de HTML5, CSS3 y JavaScript.
- Aplicativo web basado en seguridad de los usuarios

2.4.2. Requisitos comunes de las interfaces

La interfaz del usuario para el módulo blockchain no aplicará ya que al hacer contratos inteligentes no se necesitará interfaz, esta parte estará realizada por el Módulo front-end del proyecto en general.

2.4.3. Interfaces de Hardware

Es necesario disponer de equipos de cómputo que cumplan con las siguientes características mínimas:

- Adaptadores de red.
- Acceso a internet
- Procesador de 1.66GHz o superior.
- Memoria RAM mínima de 512Mb.
- Mouse.
- Teclado
- Pantalla.

2.4.4. Interfaz de software

- Sistema Operativo: Windows 7 o superior, Linux o Mac OS.
- Explorador: Mozilla, Google Chrome.
- Instalación de complemento MetaMask
- Cuenta en MetaMask

2.4.5. Funciones

Requerimientos funcionales

Cantidad de actividades	4
Actividad #1	
Nombre de la actividad	Descripción
Desarrollar el contrato inteligente	Crear el contrato inteligente por medio del lenguaje de programación solidity
Actividad #2	
Nombre de la actividad	Descripción
Conectar nodos en la blockchain	Descentralizar las cadenas de bloques de la red, esto quiere decir Realizar el contrato inteligente para la cadena blockchain aplicando el lenguaje solidity donde se automatizará las transacciones por usuario y el cifrado a cada bloque.

Actividad #3	
Nombre de la actividad	Descripción
Ejecución del contrato inteligente	Agregar el contrato inteligente en la blockchain, esta red tiene un bloque donde se inserta el contrato inteligente que es el encargado de dar instrucciones a la cadena de bloques y da la suficiente información para qué hacer con cada transacción recibida
Actividad #4	
Nombre de la actividad	Descripción
Configuración de ganache	Creación de la red blockchain por medio de este software que nos permite crear redes blockchain locales.
Actividad #4	
Nombre de la actividad	Descripción
Creación de dirección Ethereum	Se creará una cuenta en común para el desarrollo de entorno de pruebas, configurando la cuenta MetaMask

2.5. REQUERIMIENTOS NO FUNCIONALES

Cantidad de actividades	4
Actividad #1	
Nombre de la actividad	Descripción
Conexión a la blockchain	La aplicación debe contar con alojamiento de las transacciones con la información del voto realizado por los usuarios para esto será aplicada la blockchain donde se cifrará cada transacción siendo inalterable
Actividad #2	
Nombre de la actividad	Descripción
Modelado del software	En el modelado a realizar en esta sección se encuentran los siguientes - modelos o diagramas: - Diagramas de Casos de Uso. - Diagrama de Secuencia. - Diagrama de Actividades.
Actividad #3	
Nombre de la actividad	Descripción
Realización de manuales	Se debe disponer de los manuales de instalación y de usuario los cuales deben estar legibles para cualquier tipo de persona.
Actividad #4	
Nombre de la actividad	Descripción
Lenguaje solidity	Solidity es un lenguaje de alto nivel orientado a contratos. Su sintaxis es similar a la de JavaScript y está enfocado específicamente a la Máquina Virtual de Ethereum (EVM). Su IDE principal es

	remix está basado en un navegador que integra un compilador y un entorno en tiempo de ejecución para Solidity sin los componentes orientados al servidor.
Actividad #5	
Nombre de la actividad	Descripción
Truffle suite	Logra la conversión de lenguaje solidity a binario, Es un entorno de desarrollo que facilita la integración de contratos inteligente en la cadena de bloques, que nos ofrece: • Compilación, enlace y despliegue de Smart contracts desde el propio framework • Depuración y testing automatizado de contratos • Framework con scripts de despliegue y migraciones en redes públicas y privadas • Acceso a cientos de paquetes externos y gestión con EthPM & NPM

2.5.1. Requisitos de Rendimiento

Dentro de las proyecciones esperadas en cuanto al rendimiento del aplicativo, se tiene por estipulado que:

- Evitar redundancia de datos para que las transacciones en la blockchain sean más rápidas y así mismo lo suficientemente eficaz.
- se contará con el acceso de 80 estudiantes para así probar la capacidad del software en entorno a pruebas.
- El número de administradores puede oscilar entre uno (1) y diez (10), sin embargo, no es impedimento el número de usuarios con acceso y será criterio de la institución crear o no más usuarios.

2.5.2. Restricciones de diseño

- Diagrama de secuencia
- Diagrama de actividades
- Diagrama de casos de uso
- Diagrama entidad relación

2.6. ESPECIFICACIÓN DEL DISEÑO

2.6.1 Modelo de entidad relación (MER)

En este modelo se ha relacionado todo el proceso del módulo Blockchain, desde la inicialización de la red hasta el momento donde se hace la transacción a la Blockchain donde interactúa primero por el contrato inteligente para agregarse después a la cadena de bloques.

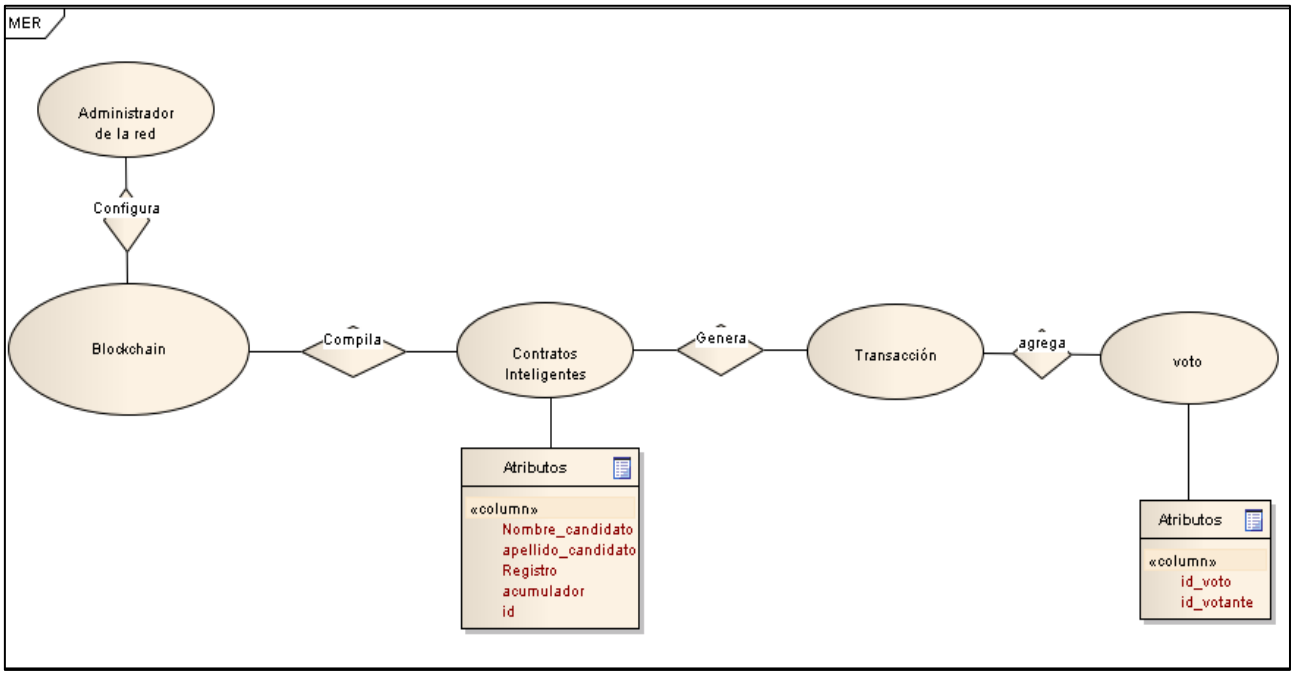


Figura 4. Modelo entidad relación

2.6.2 Roles propuestos

Tabla 5. Roles propuestos

ROL	ADMINISTRADOR
FUNCIONES	1. Ejecutar Red 2. Configurar Blockchain 3. Desplegar Smart Contract 4. Supervisar Blockchain

2.6.3 Diagrama de caso de uso

En los diagramas de caso de uso representa la forma en como un cliente opera con el sistema de desarrollo, los actores que interactúan en el sistema y sus funciones o eventos que cumplen dentro de este.

Descripción de casos de uso contrato inteligente:

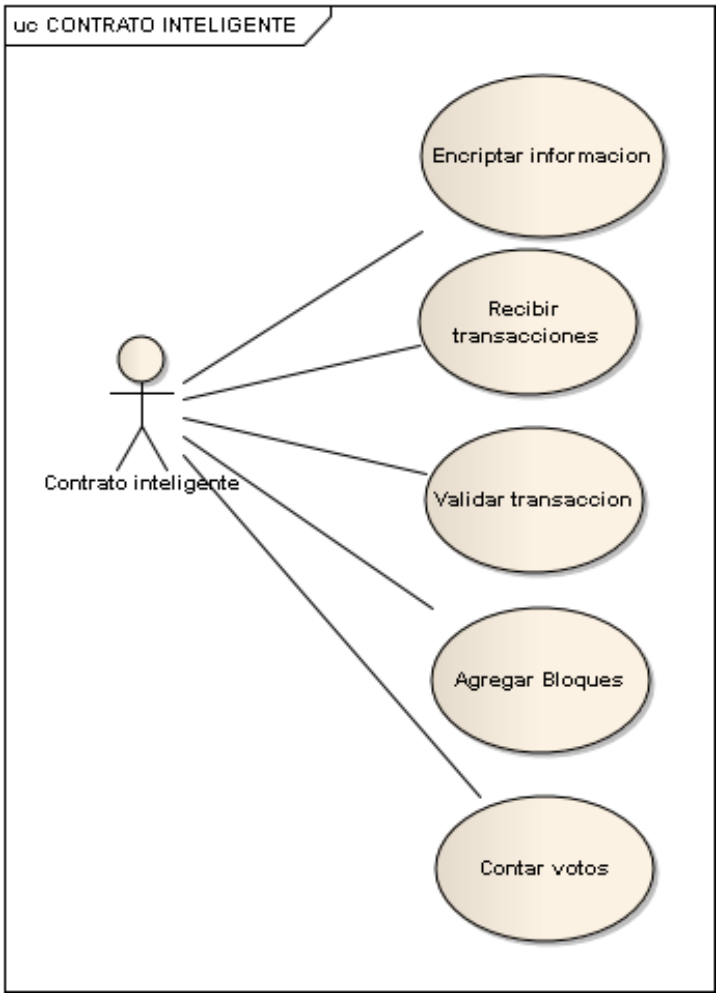


Figura 5. Caso de uso del contrato inteligente

Tabla 6. Caso de uso del contrato del contrato inteligente

Nombre	**Descripción**
Encriptar información	encriptar información acerca de los candidatos para que estos no puedan ser modificados.
Recibir transacciones	recibir la transacción hecha por los nodos de la Blockchain
Validar Transacción	valida todas las transacciones en cada uno de los nodos de la red.

Agregar bloques	agregar bloques después de validar los nodos en la red, dando validación a los contratos inteligentes
Contar votos	Contará los votos válidos para cada candidato

2.6.4. Diagramas de secuencias

Los diagramas de secuencia son una representación gráfica que resume y explica cada caso de uso presentados en el ítem anterior.

1. **Correr contrato Inteligente.**

    - **Iniciar Proceso votación:** Inicia el proceso de elecciones hasta la finalización programada.

    - **Insertar Contrato primer bloque:** AL iniciar el proceso de votación el contrato se ingresa en el primer bloque de la cadena para poder controlar los que se van añadiendo.

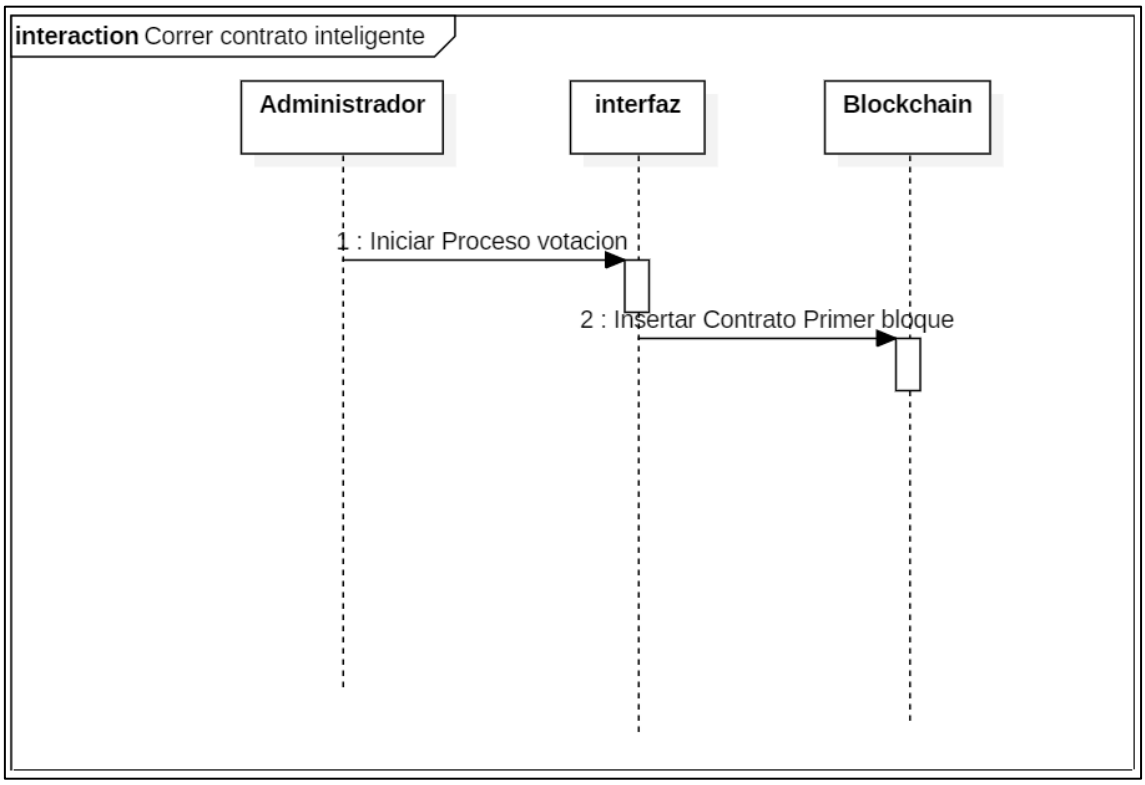


Figura 6. Diagrama de secuencia Correr contrato inteligente

2. **Informe Resultados.**
    - **Conteo de bloques:** El contrato realiza el conteo de bloques para poder dar los resultados.
    - **Cantidad de votos:** El contrato nos retorna la cantidad de votos por candidato.

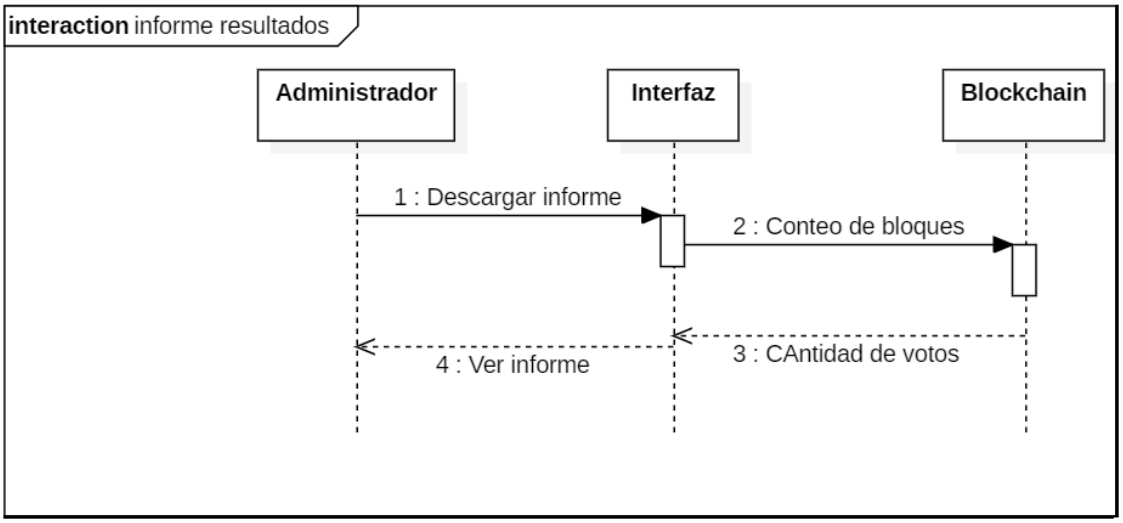


Figura 7. Diagrama de secuencia informe resultados.

3. **Supervisar Blockchain.**

    - **Monitoreo Transacciones:** El administrador puede monitorear la Blockchain.
    - **Monitor de Blockchain:** Se instala una interfaz de monitor de transacciones.
    - **Transacciones:** Retorna las transacciones en tiempo real para monitorear la cadena de bloques.

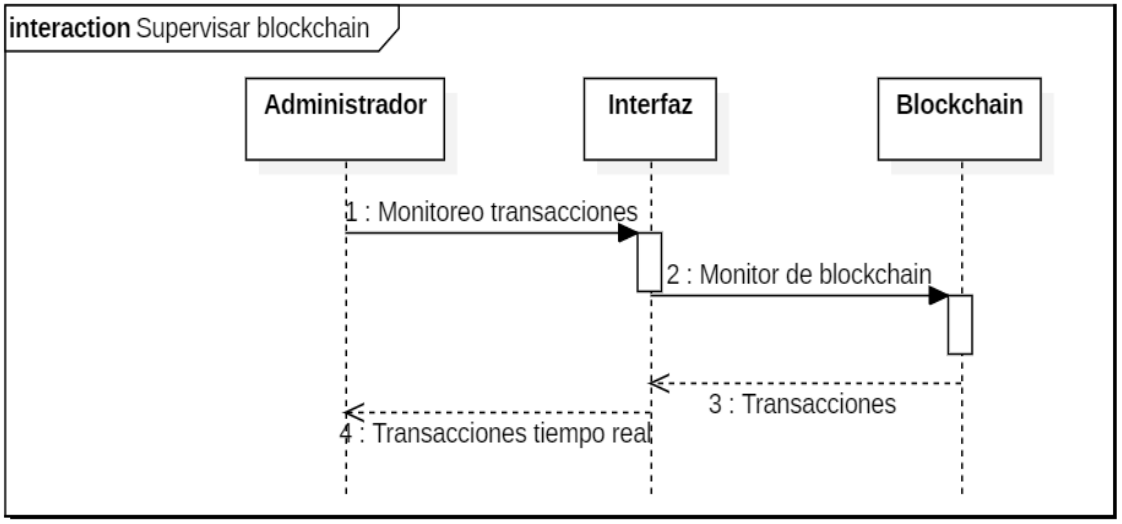


Figura 8. Diagrama de secuencia supervisar Blockchain

1. **Realizar voto.**
    - **Enviar voto:** El estudiante selecciona el candidato de su preferencia luego envía el voto.
    - **Transacción a la Blockchain:** El sistema envía la transacción a la Blockchain pasando por el contrato inteligente.
    - **Encriptación de la transacción:** El contrato se encarga de encriptar la transacción en un bloque para luego añadirlo a la cadena.

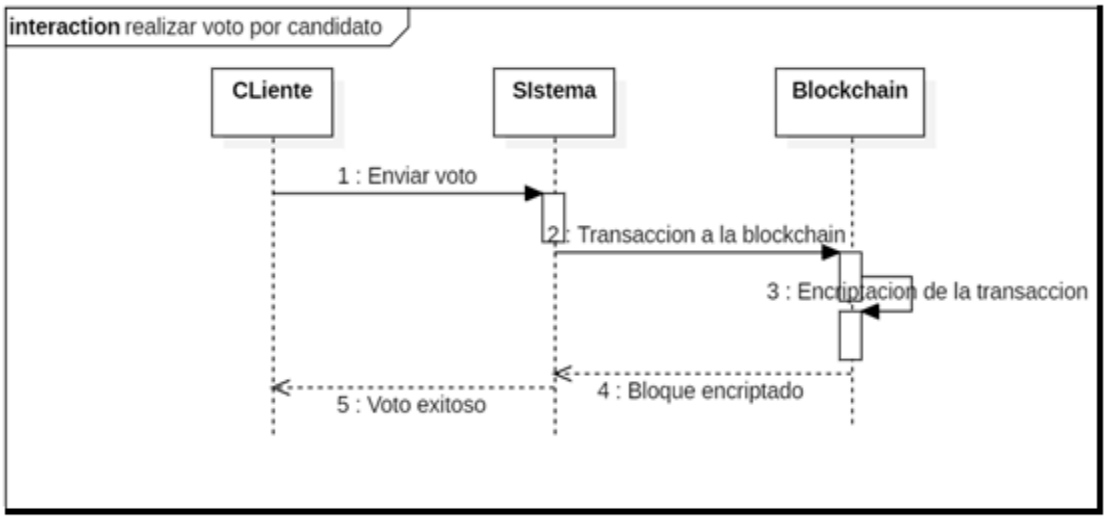


Figura 9. Diagrama de secuencia Realizar voto

Diagramas de secuencia Contrato inteligente:

1. **Conteo.**
    - **Petición:** El contrato realiza una petición de información a la blockchain para mirar la información encriptada.
    - **Acumulador:** Se crea un acumulador dentro del contrato para ir almacenando los votos.
    - **Numero Votos:** Se retorna el total de votos y la cantidad de cada candidato.

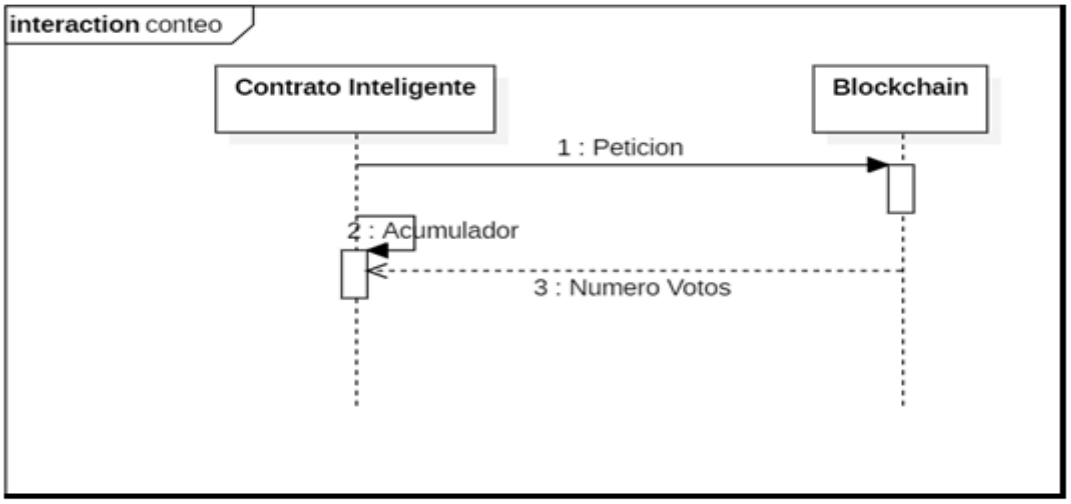


Figura 10. Diagrama de secuencia conteo

2. **Encriptar candidatos.**
    - **Insertar Contrato:** Se Inserta el contrato en el bloque génesis que es el que empieza la cadena de bloques.
    - **Creación primer bloque:** En el primero bloque va el contrato inteligente programado para realizar el comportamiento de los demás bloques.

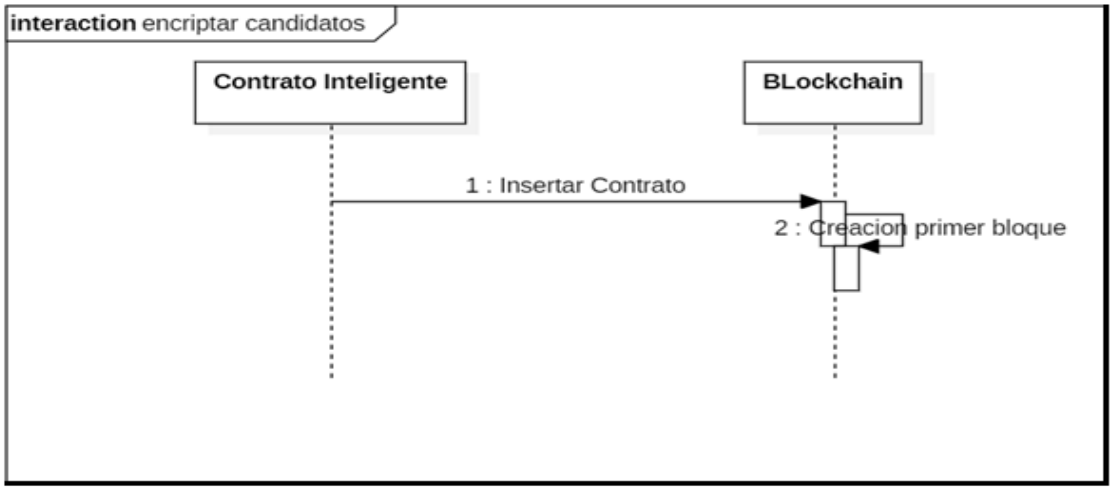


Figura 11. Diagrama de secuencia encriptar candidatos.

3. **Verificación Transacción.**
    - **Recibir transacción:** El contrato recibe las transacciones desde el backend del sistema
    - **Información de encriptación:** Se retorna el código de encriptación con el que se está realizando la cadena.
    - **Validación encriptación:** Se valida que la transacción recibida pertenezca a ese bloque por medio del código hash.
    - **Agregar nuevo bloque:** Se agrega el bloque asignándole otro código para así seguir con el proceso de cifrado de las demás transacciones.

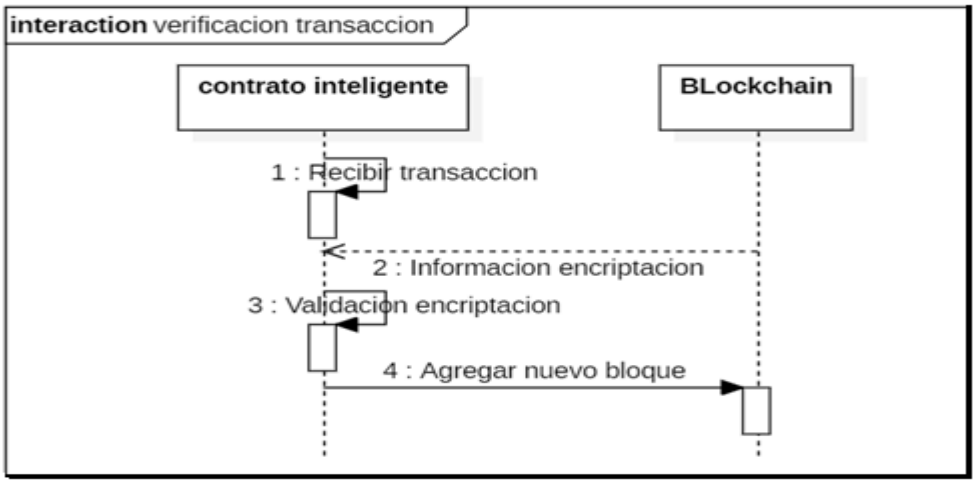


Figura 12. Diagrama de secuencia verificación de voto

2.6.5. Diagramas de actividades

En el diagrama de actividades mostramos lo realizado respecto a la estructura y funcionamiento del Smart contract y la Blockchain.

Diagrama de actividades Administrador

1) **Correr Contrato.**

- **Iniciar votación:** El administrador notifica al sistema cuando se inicia la votación.
- **Compilar Contrato:** Se compila el contrato inteligente con los candidatos registrados.
- **Bloque Génesis:** Se inserta el contrato compilado en el primer bloque de la cadena.

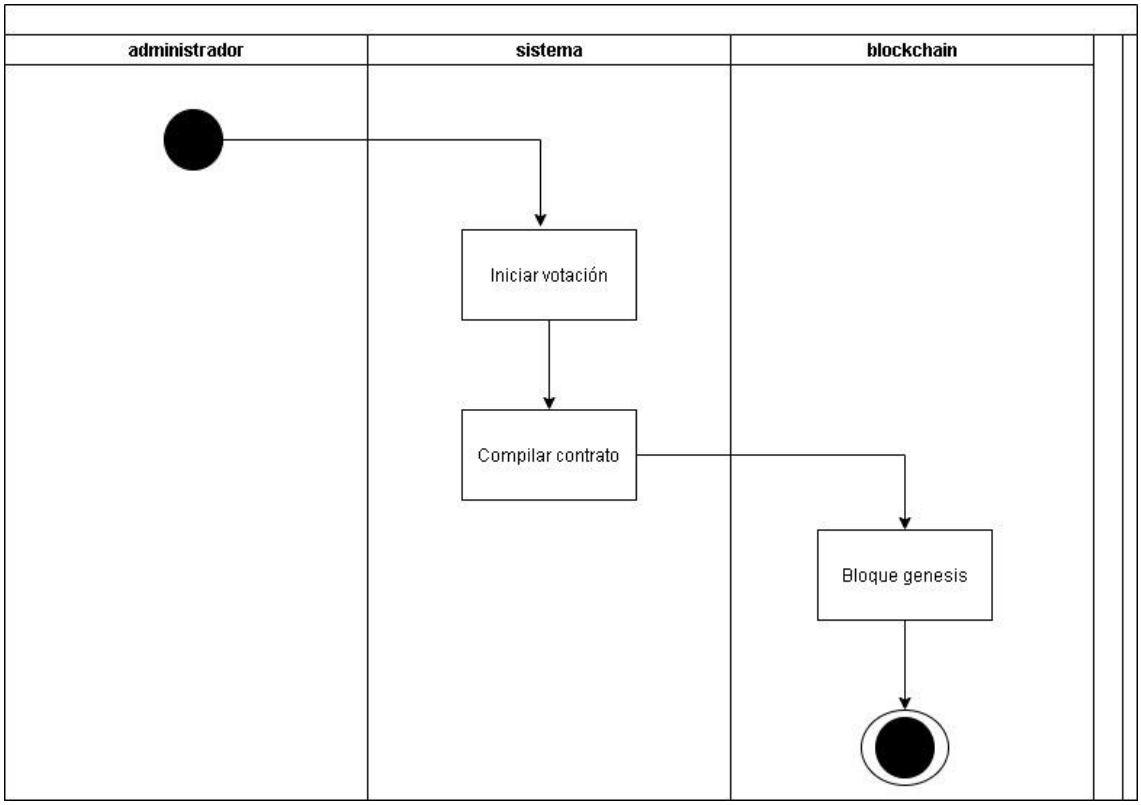


Figura 13. Diagrama de actividades correr contrato

2) **Supervisar Blockchain.**

- **Monitoreo transacciones:** Solicita la visualización de las transacciones al sistema.

- **Monitor bloques cifrados:** Con un monitor de Blockchain se analizan las transacciones.

- **Lista bloques:** Genera una lista en tiempo real donde se muestra las transacciones y los bloques cifrados con su respectivo hash.

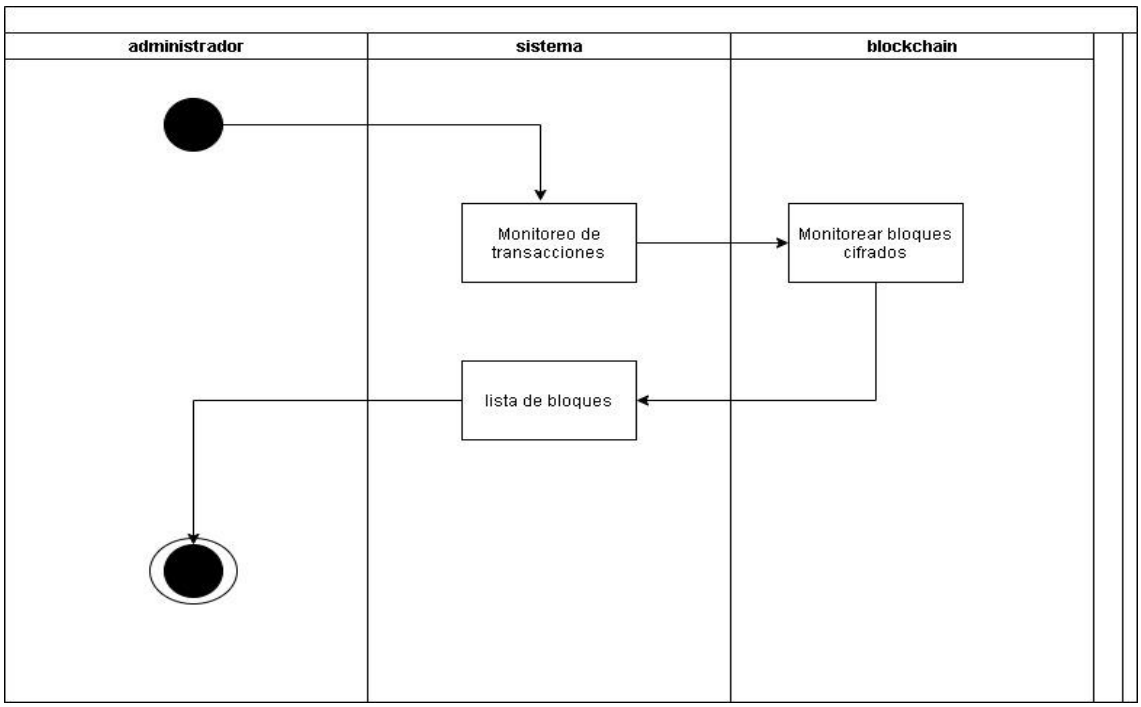


Figura 14. Diagrama actividades supervisar Blockchain

3) Informe Resultado

- **Conteo Transacciones:** El contrato realiza un coteo de los votos por bloque que encuentra cifrados.

- **Votos por candidato:** Se retorna el número de votos por candidato.

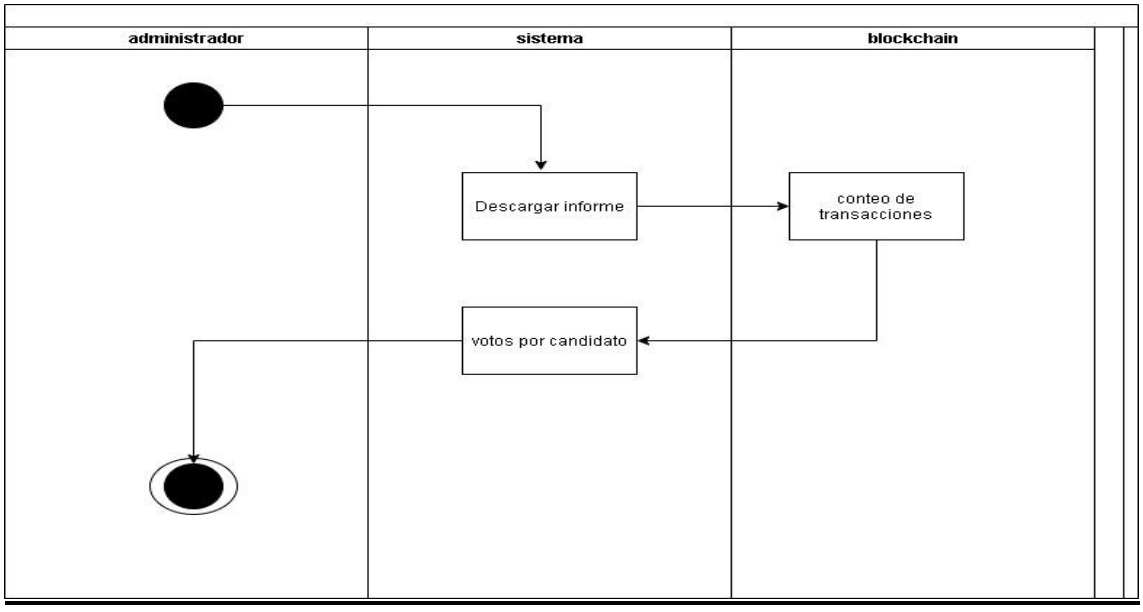


Figura 15. Diagrama de actividades Informe de resultados

Diagrama de actividades añadir bloque

1) **Realizar voto.**

- **Realizar voto:** El usuario en la interfaz de voto procede a seleccionar el candidato.
- **Transacción a Blockchain:** Se transfiere el voto al contrato inteligente.
- **Encriptar en nuevo bloque:** Se encripta la transacción que contiene los votos de los usuarios.

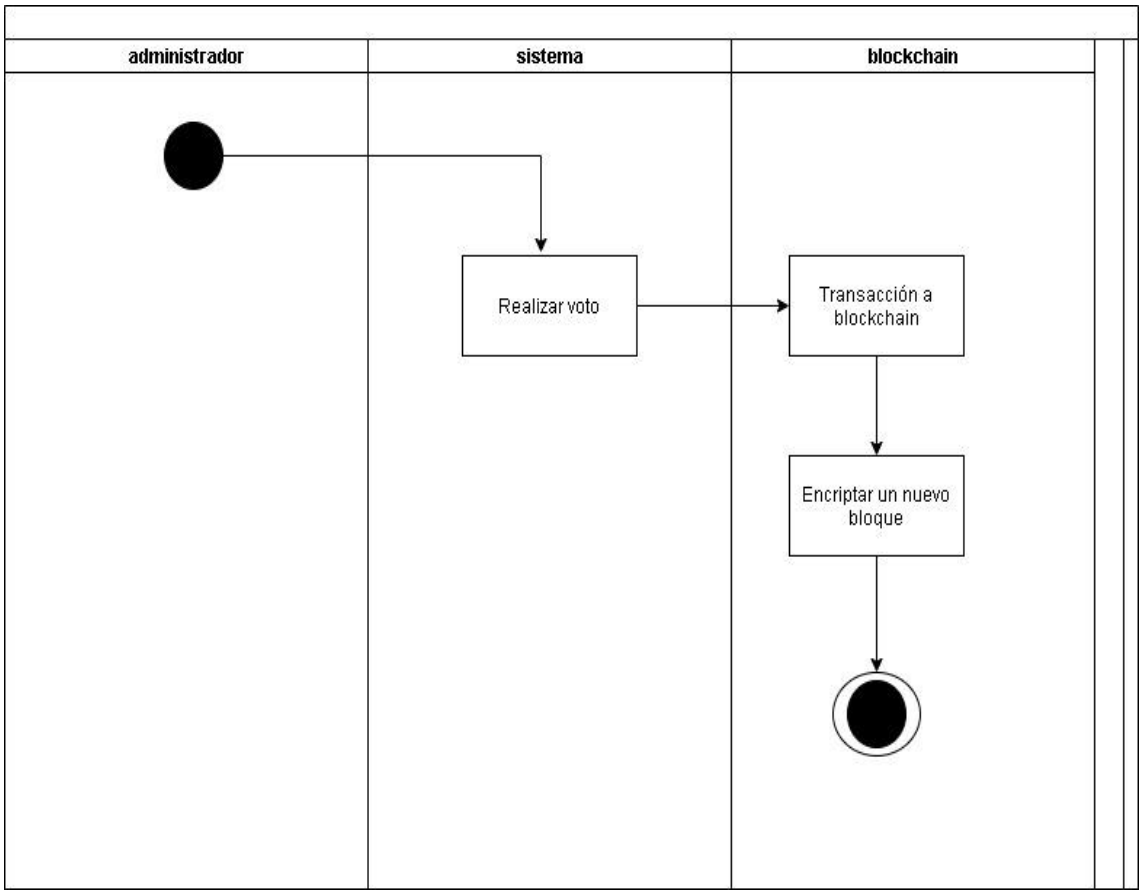


Figura 16.Diagrama actividades realizar voto.

Diagrama de actividades contrato inteligente

1) **Conteo**

- **Petición:** El contrato realiza una petición a todos los bloques para obtener su información.
- **Sumador de votos:** Con la información de cada bloque se van acumulando los votos por candidatos.
- **Resultados:** Al final el contrato tiene almacenado todos los votos del proceso de elección y la cantidad por candidato.

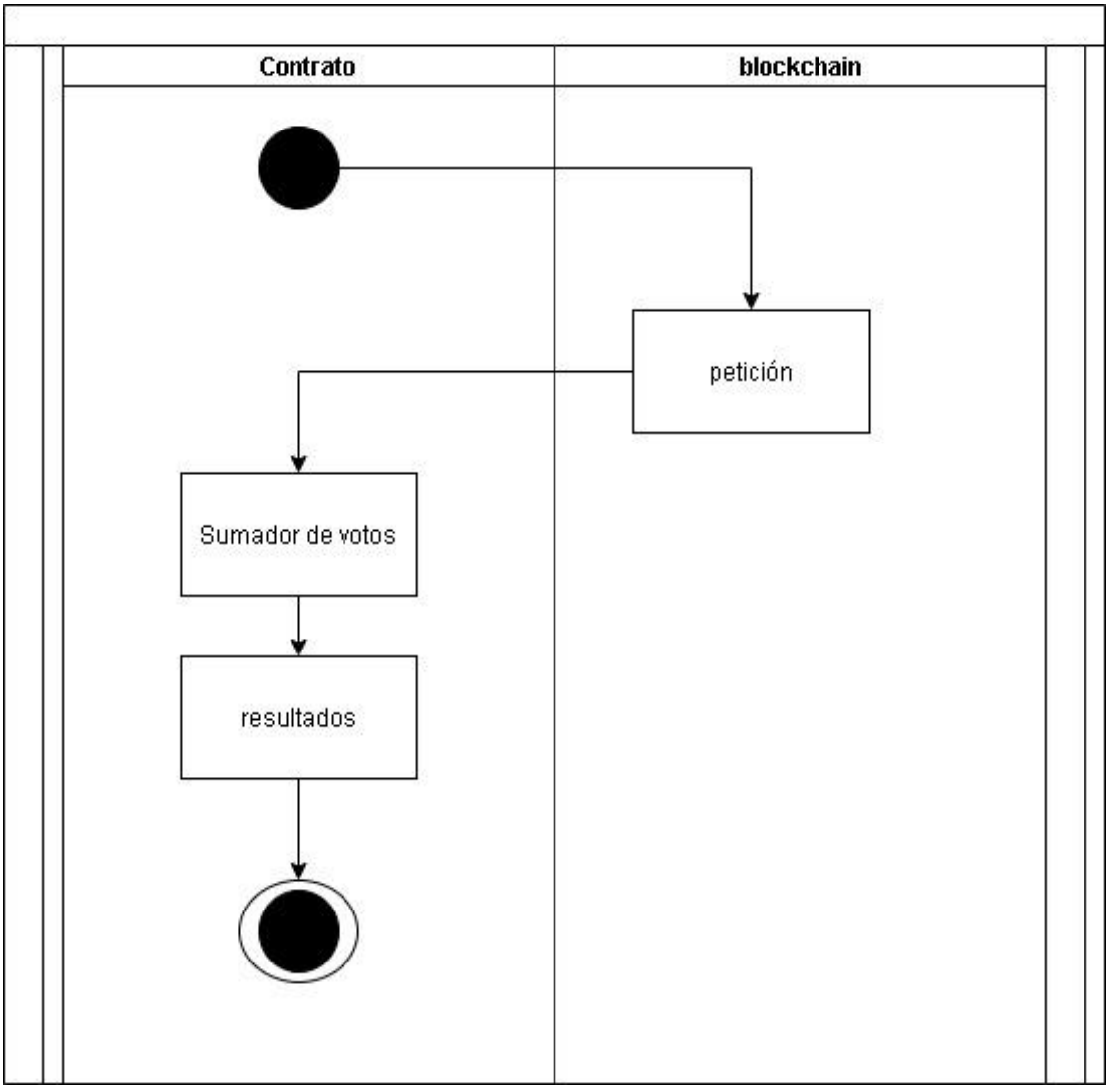


Figura 17. Diagrama actividades conteo

2) Encriptar candidatos

- **Compilar contrato:** Luego de obtener los datos de cada candidato se compila el contrato.

- **Insertar contrato:** Se inserta el contrato con los candidatos almacenados en la Blockchain.

- **Primer bloque:** Se almacena el contrato en el primer bloque de la cadena para que realice todo el procedimiento.

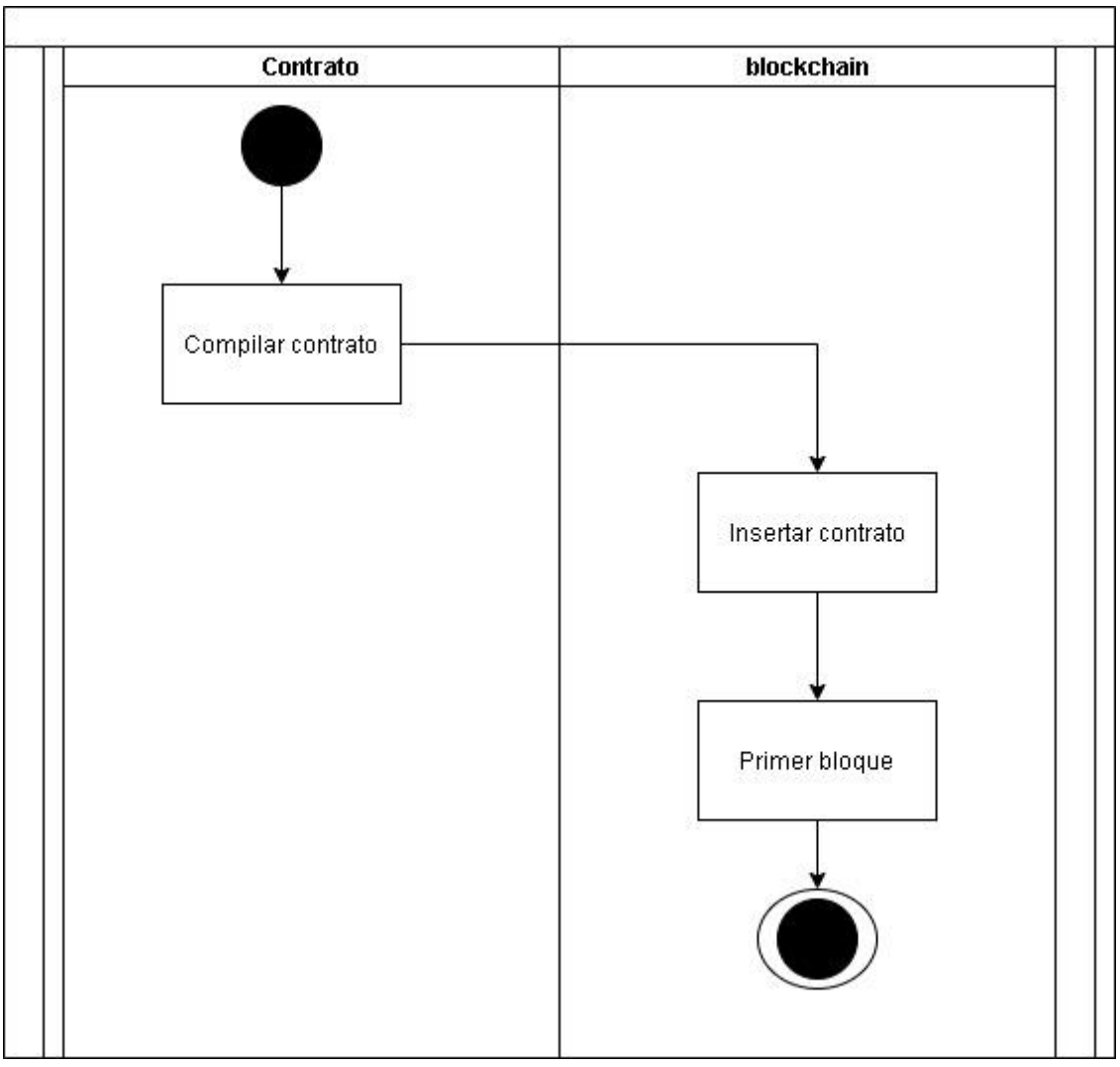


Figura 18. Diagrama actividades encriptar candidatos

3) Verificación transacción

- **Transacción:** El contrato recibe la transacción, primeramente.
- **Validar encriptación:** El contrato compara los bloques predecesores para mirar si el cifrado pertenece a esa red Blockchain.
- **Nuevo bloque:** Al corroborar que la transacción es válida se procede a encriptar y agregar un nuevo bloque a la cadena.

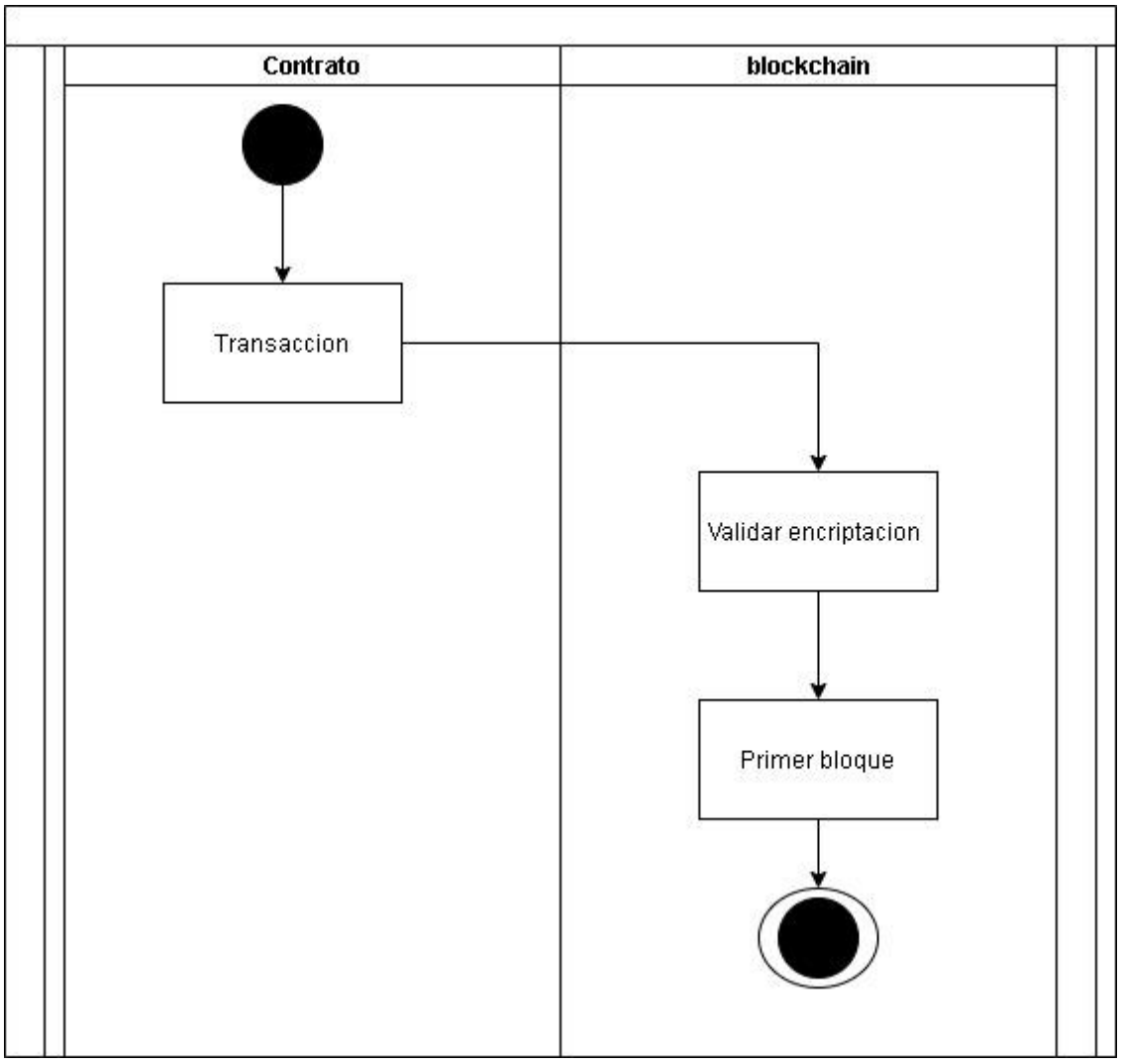


Figura 19. Diagrama actividades verificación transacción

4. Integración de módulo blockchain

- **Registro en app móvil:** El usuario debe haberse registrado previamente y a su vez debe formar parte de la universidad de Cundinamarca.

- **Autenticación del votante:** El sistema autentica al usuario.

- **Cumple credenciales:** El sistema verifica que se cumplan los requisitos para generar el código OTP que es un algoritmo criptográfico que puede crear un texto cifrado del que nadie puede obtener el texto plano y que no puede quebrarse aún con potencia de cálculo infinito e ilimitada cantidad de tiempo(Bast et al., 2017)

- **Generar código OTP:** Se genera un código único para el ingreso de la página web

- **Página principal:** Se ve la página principal

- **Lista de candidatos:** Se ven los candidatos añadidos a la votación

- **Realización del voto:** Se agregan los votos por cada candidato, el usuario solo podrá votar una vez.

- **Nodo agregado:** se agrega nodo a la cadena de blockchain

- **Reportes de votación:** al finalizar la votación se verán los respectivos reportes con los resultados de la misma.

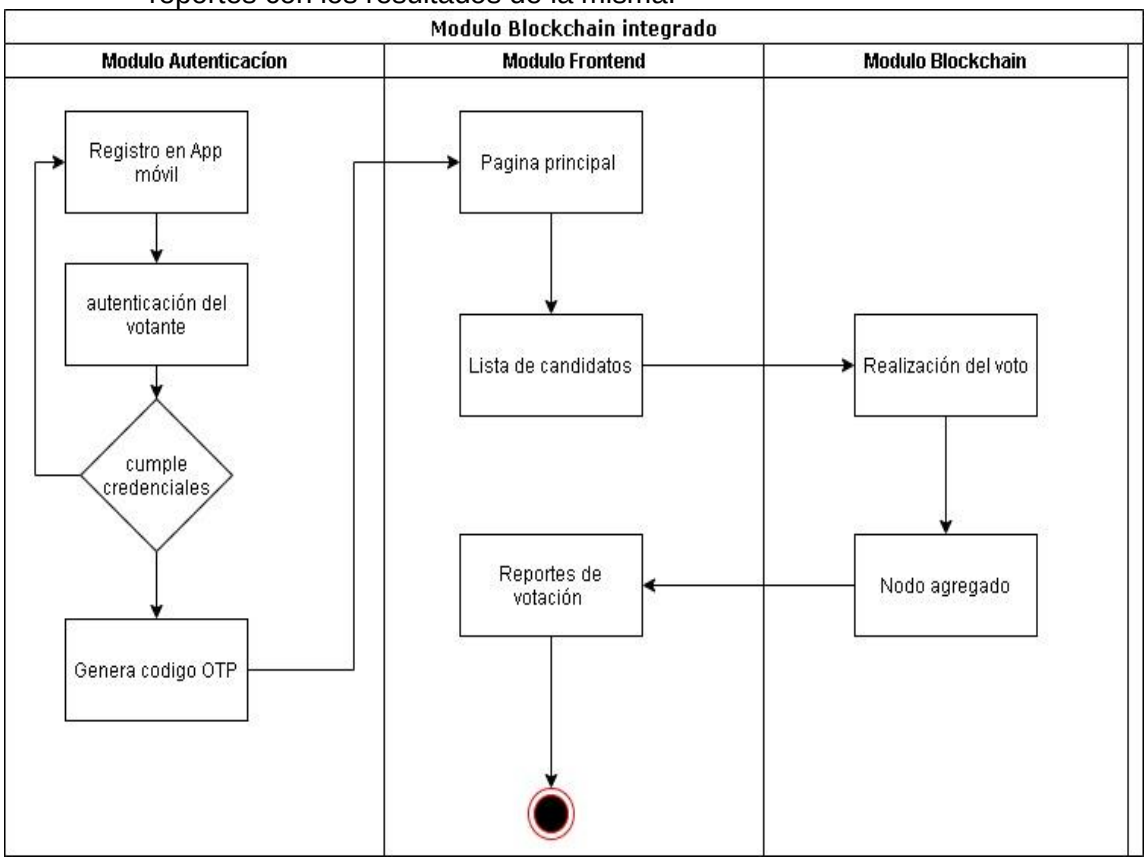


Figura 20. Diagrama de actividades de integración módulo blockchain

2.6.6. Diagrama de clases

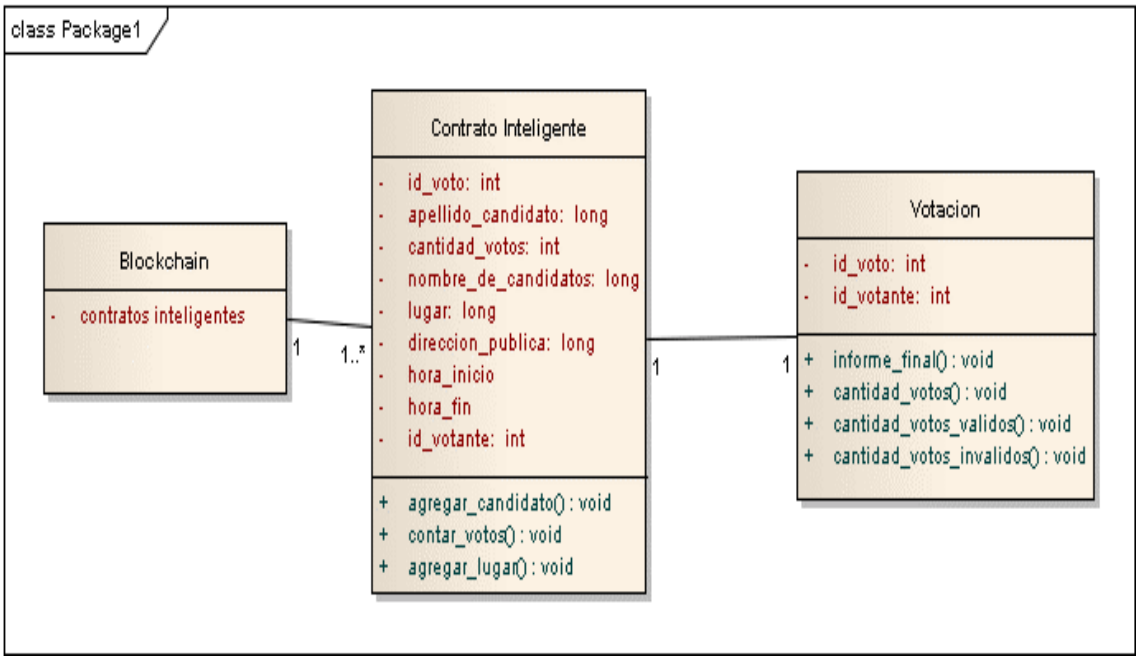


Figura 21. Diagrama de clases

2.7. RESULTADO PRUEBA SonarQube

Con el objetivo de evaluar el código JavaScript implementado en el desarrollo del proyecto titulado “SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO BLOCKCHAIN” se utilizó el software SonarQube que es una plataforma para evaluar código fuente. Es software libre y usa diversas herramientas de análisis de código fuente para detectar errores y vulnerabilidades en el código y obtener métricas que pueden ayudar a mejorar la calidad del código de un programa. SonarQube maneja un estándar de calificación para saber la calidad del código evaluado como se observa en las siguientes tablas:

Tabla 7. Criterio fiabilidad, Prueba SonarQube

Fiabilidad	
Calificación	**Criterio**
A	0 errores
B	Al menos 1 error menor
C	Al menos 1 error mayor
D	Al menos 1 error critico
E	Al menos 1 bloque de error

Tabla 8. Criterio seguridad, Prueba SonarQube

Seguridad	
Calificación	**Criterio**
A	0 vulnerabilidades
B	Al menos 1 vulnerabilidad menor
C	Al menos 1 vulnerabilidad mayor
D	Al menos 1 vulnerabilidad critico
E	Al menos 1 bloque de vulnerabilidad

Tabla 9. Criterio código duplicado, Prueba SonarQube

Código duplicado	
Calificación	**Criterio**
<1%	Alta calidad
Entre 1% - 5%	Buena calidad
Entre 5% - 25%	Razonable, pero debe corregirse
>25%	No es razonable y debe corregirse

Tabla 10. Criterio mantenibilidad, Prueba SonarQube

Mantenibilidad	
Calificación	**Criterio**
A	< = 5%
B	Entre 6% - 10%
C	Entre 10% - 20%
D	Entre 20% - 50%
E	Nada más del 50%

2.7.1. Reporte prueba SonarQube

Figura 22. SonarQube, Reporte

Como se observa en el reporte generado por SonarQube al código desarrollado por el módulo Blockchain, genera una valoración de **Aprobado** al evaluar los diferentes criterios mencionados anteriormente con la siguiente calificación:

Fiabilidad: Calificación A

Esta es la calificación más alta, el software la define cuando en el código fuente no se encuentran errores ya sean sintácticos o lógicos, esto involucra que la aplicación puede operar libre de fallos.

Seguridad: Calificación A

Esta es la calificación más alta, en este paso se evalúa la seguridad que implementa la aplicación, así mismo encuentra posibles vulnerabilidades en el código y como se evita el ataque que personas maliciosas puedan hacer a la aplicación.

Mantenibilidad: Calificación A

Esta es la calificación más alta, en este paso se evalúa la capacidad que tiene el software para ser modificado y adaptarse a nuevas funcionalidades, también pueden ser correcciones o mejoras en futuras versiones del código.

Duplicados: Calificación Alta Calidad

El análisis de código duplicado permite encontrar bloques duplicados en el código fuente, este resultado permite observar que en el código desarrollado no hay duplicidad de código.

- **Análisis NVivo**

  NVivo es una aplicación diseñada para el análisis de datos cualitativos que pueden encontrarse en diversidad de recursos, tales como entrevistas, encuestas con preguntas abiertas y cerradas, videos, audios, imágenes, así como también artículos y libros. Permite almacenar, organizar y obtener informes o resúmenes de los datos más importantes que surgen del análisis realizado (Fuentes Vergara).

  Para el análisis cualitativo del módulo blockchain se implementaron entrevistas en Google Forms, las cuales fueron realizadas a estudiantes de la universidad de Cundinamarca que usaron la aplicación y de la misma manera el acceso a la plataforma web, donde expresan su opinión acerca de los aspectos más relevantes del sistema. Las preguntas realizadas por el módulo blockchain se presentan a continuación:

Tabla 11 Preguntas, NVivo

Preguntas
¿Cree usted que el Sistema de votación web basado en Blockchain es seguro? y ¿Por qué?
¿Cree usted que el Sistema de votación web basado en Blockchain reducirá el fraude en la política colombiana? y ¿Por qué?
¿Qué opina al ejercer su derecho al voto a través del Sistema de votación web basado en Blockchain?
¿Cuáles ventajas observa al ejercer su derecho al voto a través del Sistema de votación web basado en Blockchain?

Como primer paso del análisis se utilizó la herramienta de consulta de palabras frecuentes que ofrece NVivo para obtener las palabras que más se repitieron, esta permite generar una imagen donde las más grandes tienen mayor relevancia, así como se muestra a continuación:

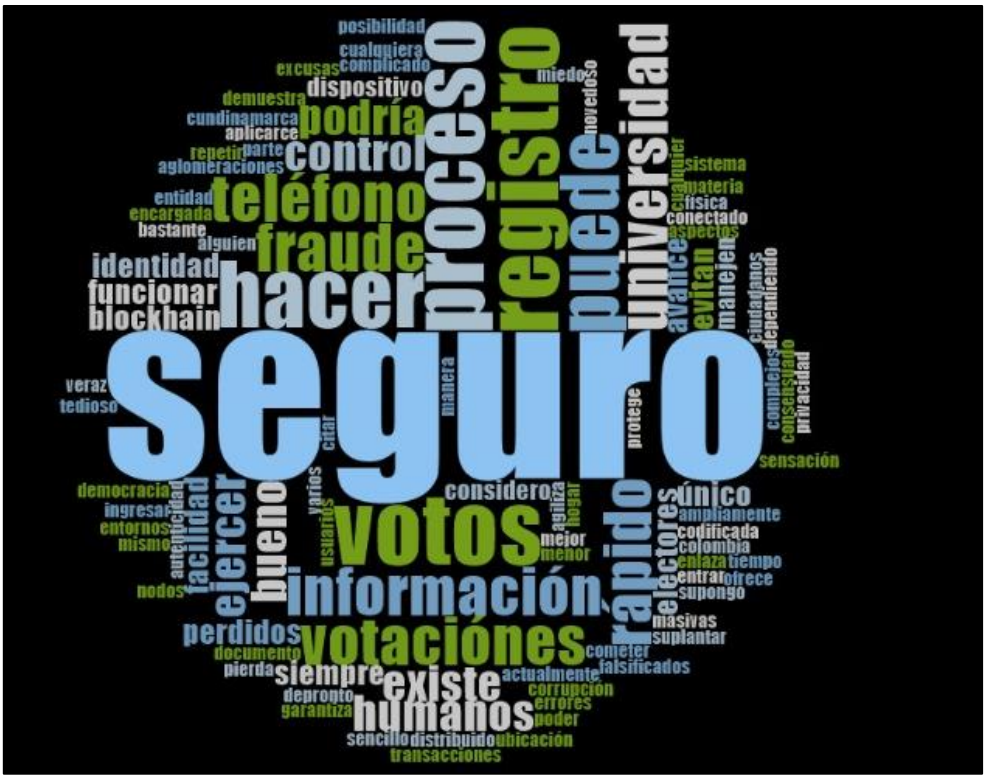


Figura 23. Palabras NVivo

Como se puede observar en la imagen las palabras con más relevancia que repitieron los estudiantes de la universidad de Cundinamarca en las entrevistas para emitir su opinión fueron información, votación, seguro, fraude, estas palabras van asociadas al proceso de votación usando blockchain.

NVivo cuenta con la herramienta de Nodos que actúan como contenedores de las referencias (segmentos de texto) asociadas con una misma categoría que pueden provenir de diferentes recursos, es la clasificación que se considera más importante para el análisis, permite generar un libro de códigos que actúa como glosario que ayuda a entender de manera más explícita que referencias deben ir asignadas en cada categoría.

Tabla 12. Libros de código de NVivo

Nombre	Descripción
Votación	Mecanismo mediante el cual se puede elegir y ser elegido mediante el voto
Seguro	Se encuentra libre de peligro o riesgo
Fraude	Engaño económico con la intención de conseguir un beneficio, y con el cual alguien queda perjudicado

Información	Conjunto de datos organizados que tienen un objetivo común
Registro	Acción de anotar un suceso en algún lugar, que requiere de dejar evidencia de un acontecimiento

El libro de códigos presenta la estructura general de los nodos que permitirán realizar la clasificación y codificación de las entrevistas para posteriormente generar el análisis y encontrar opiniones en común, estos nodos también se pueden organizar por jerarquía

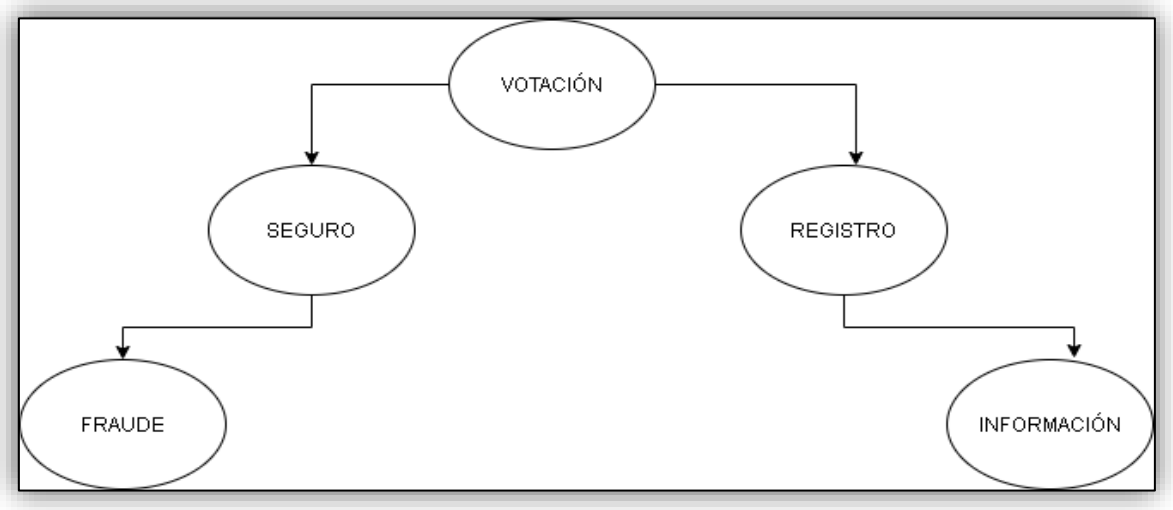


Figura 24. Jerarquía de nodos

En la figura 24 NVivo brinda la posibilidad de generar una comparación nodos versus recursos en la matriz de marcos de trabajo y así concluir las opiniones que tienen los estudiantes de la universidad de Cundinamarca sobre los temas relacionados en los nodos para concluir los aspectos más relevantes del sistema.

Tabla 13. Matriz, NVivo

SEGURO	FRAUDE	REGISTRO	INFORMACION
Si porque es un registro único, consensuado y distribuido en varios nodos de una red	Si, al ser un registro único no se podrá registrar dos o más votos con el mismo número de documento de identidad	Un proceso seguro	La información siempre estará codificada en las transacciones de red
Sí, porque tiene verificación	Sí, porque no se puede suplantar identidades para repetir votos	Es más práctico y rápido	Tiempo y seguridad
Sí, porque le da una veracidad al voto, es decir, la persona que se registre debe ser de la universidad de Cundinamarca	Dependiendo de quienes manejen esa parte, el fraude es algo muy complicado en este país	Mi voto es veraz	Demuestra que el voto es de alguien de la universidad y no cualquiera podría entrar y votar para hacer fraude

Si, el blockchain protege la información y no existiría la posibilidad de votos falsificados ni de votos perdidos	Si, actualmente hay corrupción en las votaciones, con el blockchain se garantiza el voto de los ciudadanos	Es mucho más ágil, desde su hogar la puede realizar sin miedo a que el voto de pierda	Autenticidad de voto.
Sí, es ampliamente utilizado en el mundo	No, para aplicarse a votaciones en la universidad puede funcionar, pero no sería seguro en votaciones masivas	Creo que la sensación de seguridad es menor pero el proceso mucho más rápido	Es más rápido, es mejor que ir hasta una ubicación física a votar
Si porque es muy privado su manejo	Si porque evitaría errores humanos que crean excusas para cometer fraudes electores	Muy bueno porque es un avance para la Universidad y tal vez para el país en materia de democracia	Facilidad en el proceso, entornos seguros controlados por la entidad encargada, se evitan aglomeraciones

Como se puede observar en la matriz anterior los estudiantes de la universidad de Cundinamarca tienen una opinión parecida en cuanto al sistema, la información que se presenta es clara, organizada y coherente, es un sistema que puede generar impacto positivo en los usuarios que puedan acceder a él.

2.7.2. Estimación de recursos

La estimación de los recursos requeridos para establecer el costo total del desarrollo que permite la realización del módulo Blockchain se especifica en los siguientes puntos.

Estimación evaluando los casos de uso

Esta técnica evalúa los actores y casos de uso que se plantean en el modelado UML. A los casos de uso se les asigna una complejidad basada en transacciones (interacción usuario-maquina), mientras que a los actores se les asigna una complejidad basada en su tipo, además maneja dos ítems conocidos como factor ambiental que evalúa las habilidades y entrenamiento del grupo desarrollador y el factor de complejidad técnica que consiste en la cuantificación de un conjunto de factores que pueden o no influir en el sistema a desarrollar (Arias Rojas & Chia Rodriguez, 2019).

Clasificación de los actores

La cantidad de actores presentes en el sistema y en la complejidad que se le sea asignada determina si se trata de una persona o de otro sistema quien interactúa con el software.(Arias Rojas & Chia Rodriguez, 2019).

Tabla 14. Actores

Actor	Peso	Tipo de interacción
Usuario general (modulo-front-end)	1	Complejo

Clasificación de los casos de uso

Los casos de uso se clasifican de acuerdo con la cantidad de transacciones que estos requieran:

Un caso de uso simple (**peso=5**) es aquel que posee 3 o menos transacciones; Uno medio (**peso=10**) es el que posee de 4 a 7 transacciones y un caso de uso complejo (**peso=15**) es el que posee más de 7 transacciones (Greiner, Demchum, Dapozo, & Estayno, 2010).

Tabla 15. Clasificación de casos de uso

Casos de uso	Peso	Clasificación (Número de transacciones)
Encriptar información	5	Simple
Recibir transacciones	5	Simple
agregar bloques	10	complejo
Contar votos	5	Simple

Cálculo de los factores de entorno

Después de tener en cuenta los factores técnicos para el ajuste de los Puntos de Caso de Uso, también hay que contabilizar la complejidad de los factores del entorno a cada factor se le asigna un valor entre 0 y 5 dependiendo de la influencia del proyecto. (Sanchez Sabido, 2014)

Tabla 16. Factor de entorno

Factor de entorno		Peso	Influencia
1	Familiaridad con el modelo de proyecto usado	1,5	1
2	Experiencia en la aplicación	0,5	0
3	Experiencia en programación solidity	1,5	5
4	Capacidad del analista líder	0,5	4
5	Motivación	1	4
6	Estabilidad de los requerimientos	2	2
7	Personal media jornada	-1	1
8	Dificultad en lenguaje de programación	-1	4

Cálculo de las horas de trabajo

UAW (total de peso de actores) = 1
UUCW (total peso casos de uso) = (20 x 5) + 5 + 10 =120
UUCP = UAW + UUCW
UUCP = 1+120 = 121

TCF (total factores técnicos) = 0,6 + [0,01 $* \sum_{i=1}^{i=13}(peso_i * influencia_i)$]
TCF = 0,6 + 0,355
TCF = 0,955

EF (total factores entorno) = 1,4+ [-0,03$*\sum_{k=1}^{k=8}(peso_i * Influencia_i)$]
EF = 1,4 +(-0,03 $*$ 11,5)
EF =1,055

UCP (puntos de casos de uso) = UUCP * EF * TCF
UCP = 124 * 1,055 * 0,955
UCP = 124,9

ETotal (Esfuerzo) = UCP * CF
CF = Factor de conversión (20 horas-hombre por defecto)
ETotal = 2,498 horas

- **Cálculo de esfuerzo total**

TDesarrollo (tiempo desarrollo) = ETotal **/** CHTotal
CHTotal = cantidad de hombres (2 desarrolladores)
TDesarrollo = 2,498 **/** 2
TDesarrollo = 1,249

- **Considerando que se trabajó 10 horas diarias**

TDesarrollo = TDesarrollo **/** 10 horas/día
TDesarrollo = 1,249 **/** 10 horas/día
TDesarrollo = 124 días aproximadamente

- **Cálculo del costo**

Costo Total = ETotal * 2 * TH (Tarifa por hora)
Costo Total = 2,498 * 2 * $10000
Costo Total = $49.976.000 COP

El costo total de desarrollar el proyecto es de **$49.976.000 COP** con un tiempo de desarrollo invertido de **2,498 horas** trabajando **10 horas diarias**, se aproxima a un tiempo de **8 meses** que fue el previsto desde la aprobación del proyecto

FINANCIACIÓN (FUENTES)

Tabla 17. Financiación (Fuentes)

TIPO DE FUENTE (*)	FUENTE (+)	VALOR APORTADO (en efectivo y/o especie)
Externa	Recursos personales	$2’000.000

RESUMEN POR RUBROS

Tabla 18. Resumen por rubros

Rubros	Efectivo personal	Contrapartida en especie		Total
		UDEC	Otras Entidades	
PERSONAL	$0	-	-	$0
EQUIPOS	$2’000.000	-	-	$2’000.000
MATERIALES E INSUMOS	$85.000	-	-	$85.000
SERVICIOS TECNOLOGICOS	$0	-	-	$0
VIAJES	$0	-	-	$0
OTROS	$0	-	-	$0
TOTALES	$0	-	-	$0

DETALLE DE RUBROS

Descripción de personal

Tabla 19. Descripción de personal

Nombre	Función en el proyecto	Tipo de vinculación	Dedicación Horas/semana	Entidad a la que pertenece	Solicitado en efectivo a UDEC	Contrapartida en especie		Total
						UDEC	Otras	
Cesar Barahona	Investigador principal	Docente	6 horas	Universidad de Cundinamarca	$0	-	-	$0
Daniel Barreto	Investigador auxiliar y desarrollador	Estudiante pregrado	10 horas	Universidad de Cundinamarca	$0	-	-	$0
Julian Vallejo	Investigadora auxiliar y desarrollador	Estudiante pregrado	10 horas	Universidad de Cundinamarca	$0	-	-	$0

Descripción de equipos

Tabla 20. Descripción de equipos

Descripción	Justificación	Cantidad	Valor Unitario	Solicitado en efectivo a UDEC	Contrapartida en especie		Total
					UDEC	Otras	
Portátil HP	Herramienta de trabajo	2	$2’000.000	$0	-	-	$4’000.000

Descripción de materiales e insumos

Tabla 21. Descripción de materiales e insumos

Descripción	Justificación	Cantidad	Valor Unitario	Solicitado en efectivo a UDEC	Contrapartida en especie		Total
					UDEC	Otras Entidades	
Papelería	Documentación	0	$100.000	$0	-	-	$100.000

Descripción de servicios tecnológicos

Tabla 22. Descripción de servicios tecnológicos

Descripción	Justificación	Valor	Entidad	Solicitado en efectivo a UDEC	Contrapartida en especie		Total
					UDEC	Otras Entidades	
N/A	-	$0	-	$0	-	-	$0

Descripción de viajes

Tabla 23. Descripción de viajes

Lugar/justificación	No. días	No. personas	Cantidad	Valor Unitario	Solicitado en efectivo a UDEC	Contrapartida en especie		Total
						UDEC	Otras Entidades	
N/A	0	0	0	$0	$0	-	-	$0

Descripción de otros

Tabla 24. Descripción de otros

Descripción	Justificación	Cantidad	Valor Unitario	Solicitado en efectivo a UDEC	Contrapartida en especie		Total
					UDEC	Otras Entidades	
N/A	-	0	$0	$0	-	-	$0

2.8. RESULTADOS

Los resultados que se obtuvieron en el desarrollo del módulo Blockchain del sistema de voto electrónico para los cuerpos colegiados de la universidad de Cundinamarca, fueron los siguientes:

El Smart Contract o Contrato Inteligente para realizar el proceso de votación que se observa en la Figura 25 en el que se establecen una serie de funciones para posteriormente ser agregado a la Blockchain.

```
pragma solidity ^0.5.16;

contract Voting {

    // Estructura del candidato
    struct Candidate {
        uint id;
        string name;
        uint voteCount;
    }

    mapping (uint => Candidate) public candidates;

    mapping(address => bool) public voters;

    uint public candidatesCount;

    event votedEvent(
        uint indexed _candidateId
    );

    //Constructor
    constructor () public {
    }

    // Agregar Candidato
    function addCandidate(string memory _name) public {
        candidatesCount ++;
        candidates[candidatesCount] = Candidate(candidatesCount,_name, 0);
    }

    // Votar
    function vote(uint _candidateId) public {

        require(_candidateId > 0 && _candidateId <= candidatesCount);
        candidates[_candidateId].voteCount ++;

    }

}
```

Figura 25. Resultados, desarrollo Smart Contract

Al iniciar el proyecto la blockchain tiene 0 bloques (BLOCK) como se evidencia en la Figura 26. Esto quiere decir que los contratos aún no se han implementado en la Blockchain

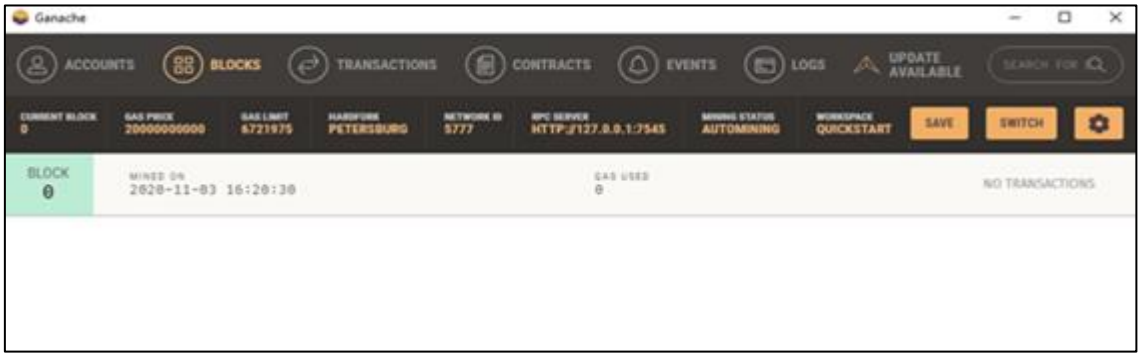


Figura 26. Resultados, Blockchain cero bloques

Una vez integrados los Smart Contracts a la Blockchain estos se verán reflejados como nuevos bloques que permiten identificar la correcta integración de los Smart Contracts en la Blockchain como se observa en la Figura 27.

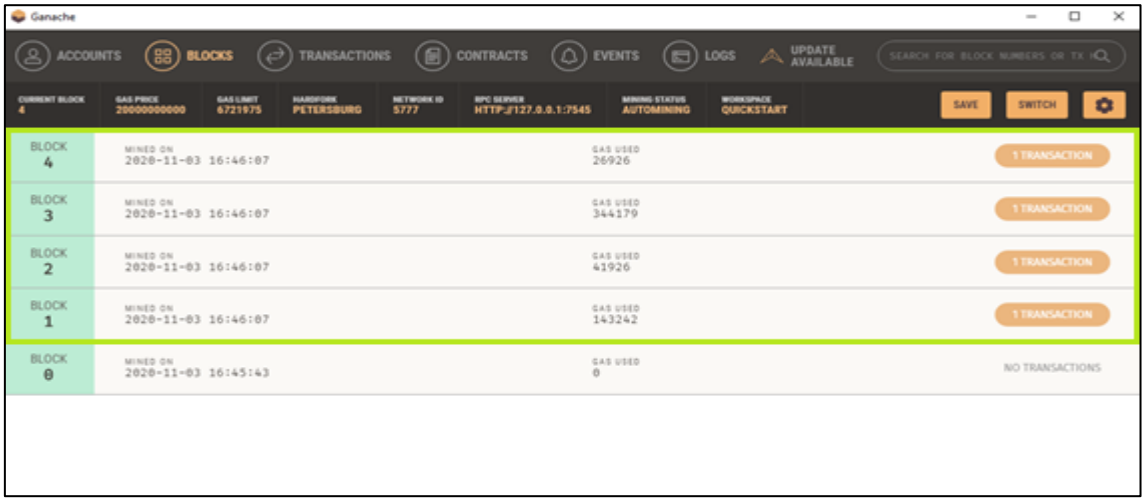


Figura 27. Resultados, Blockchain implementando los Smart Contracts

La comunicación con el módulo de Web del proyecto sistema de voto electrónico para los cuerpos colegiados de la universidad de Cundinamarca se realiza mediante servicios REST; Los servicios que implementa el módulo Blockchain permiten llevar a cabo el proceso de votación de manera segura, los servicios implementados en el proceso de comunicación son:

1. Agregar un candidato.
2. Saber la cantidad de candidatos registrados para el proceso de votación.
3. Votar.
4. Consultar el número de votos obtenidos por un candidato específico.

Para verificar el correcto funcionamiento de estos servicios se implementa la herramienta Postman que permite crear peticiones y así poder observar el correcto funcionamiento de cada servicio anteriormente mencionado.

1. Agregar Candidato: Como se observa en la Figura 28, se ingresa un nombre y una cuenta de Blockchain y como resultado devuelve un código (200 OK) lo que indica que el servicio se realizó correctamente.

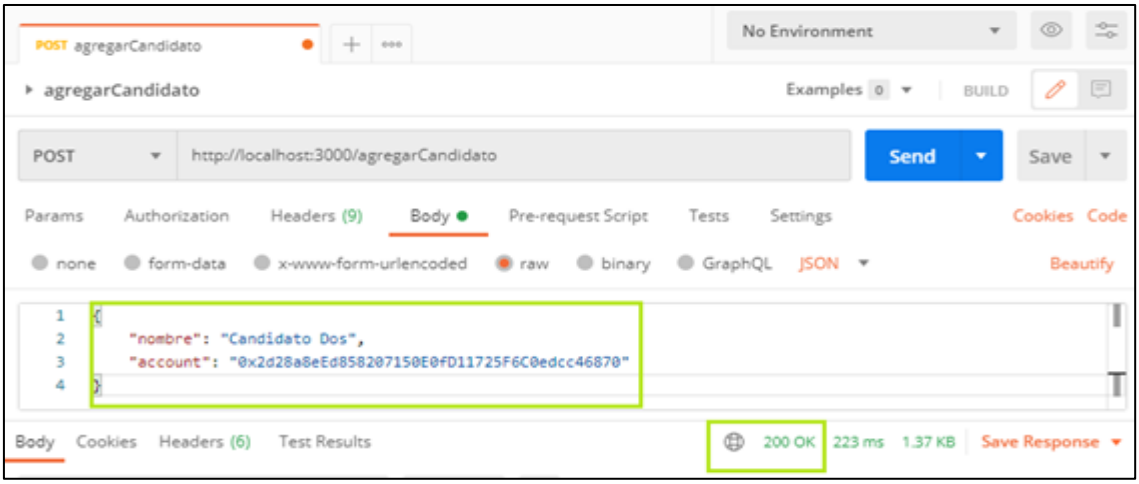


Figura 28. Resultados, Servicio agregar candidato

2. Saber la cantidad de candidatos registrados para el proceso de votación: Este servicio de igual manera devuelve un código (200 OK) como se observa en la Figura 29. Lo cual indica que fue exitoso, además muestra la cantidad de candidatos registrados para el proceso de votación.

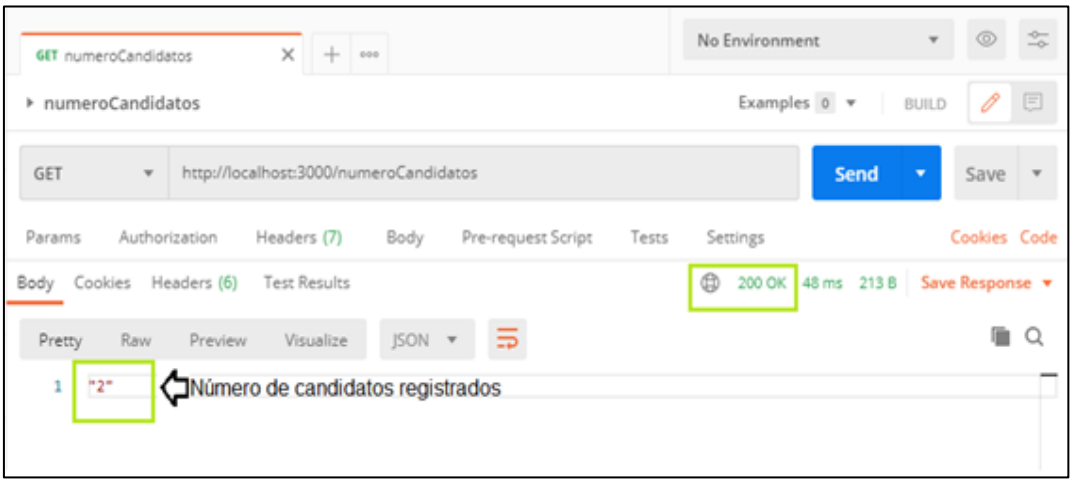


Figura 29. Resultados, Servicio número de candidatos

3. Votar: Como se observa en la Figura 30 se ingresa el id del candidato por el cual se quiere votar y una cuenta de Blockchain y como resultado devuelve un código (200 OK) lo que indica que el servicio se realizó correctamente.

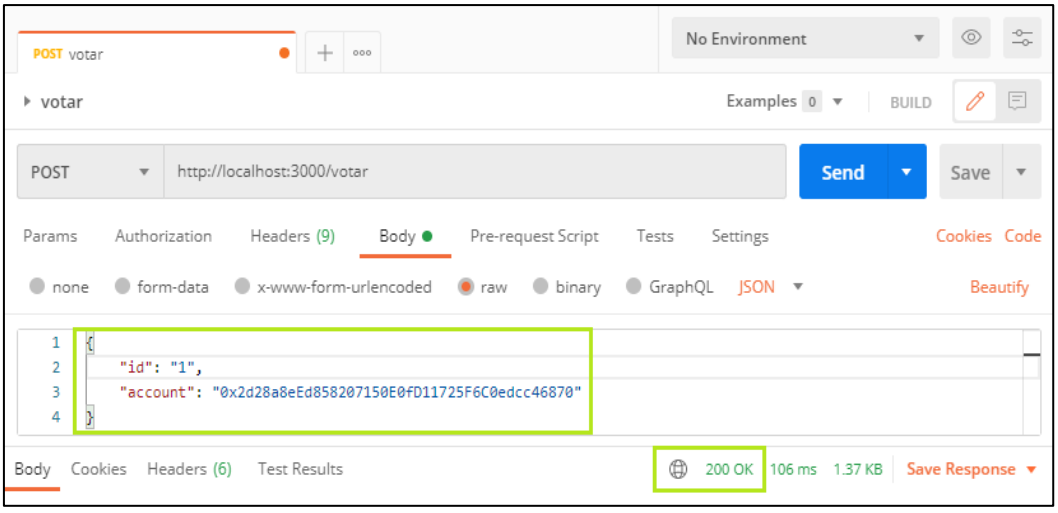


Figura 30. Resultados, Servicio votar

4. Consultar el número de votos obtenidos por un candidato específico: Este servicio de igual manera devuelve un código (200 OK) lo que indica que se realizó correctamente además del nombre del candidato del cual se quiere saber su información con la cantidad de votos obtenida como se observa en la Figura 31:

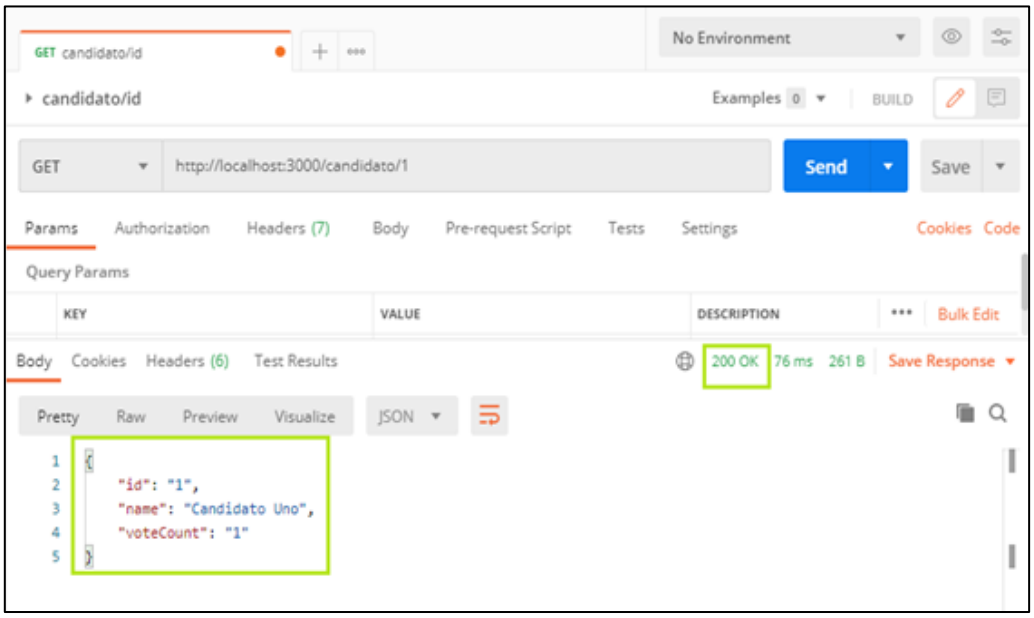


Figura 31. Resultados, Servicio consultar información del candidato

2.8.1. CONCLUSIONES Y RECOMENDACIONES

El desarrollo del proyecto titulado “SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO BLOCKCHAIN” basándose en la metodología mixta dio como resultado la realización del modelado UML, la definición de los requerimientos llevados a cabo con el formato IEEE cumplieron con los lineamientos establecidos en el cronograma en el tiempo que se estableció; para llevar una correcta codificación en el desarrollo del proyecto se realizaron reuniones en las cuales se aclaraban dudas y se hacían correcciones tanto en la documentación como en la codificación lo cual permitió completar el proyecto.

El sistema permite llevar a cabo el proceso de votación de forma segura, transparente y clara gracias a las propiedades de los Smart Contracts implementando la red Blockchain Ganache, este sistema garantiza la seguridad y la integridad de los votos al almacenarse la información en la Blockchain.

Implementar la red Blockchain y los Smart Contracts aumentan la seguridad de la información de los votos y brindan una alternativa para llevar a cabo una votación descentralizada en la que se agilizarán procesos generando solución a los problemas de corrupción y ofreciendo mayor integridad a la información del voto.

2.8.2. REFERENCIAS

Acosta, I., Nieto, E., & Barahona, C. (2015). Metodología para la evaluación de calidad de los productos software de la Universidad de Cundinamarca. *ENGI Revista Electrónica de La Facultad de Ingeniería*, *3*(2), 4. http://webcache.googleusercontent.com/search?q=cache:hPdc3fbYpooJ:revistas_electronicas.unicundi.edu.co/index.php/Revistas_electronicas/article/download/157/152+&cd=2&hl=en&ct=clnk&gl=co

Bartolomé Pina, A. R., Bellver Torlà, C., Castañeda Quintero, L., & Adell Segura, J. (2017). Blockchain en Educación: introducción y crítica al estado de la cuestión. *Edutec. Revista Electrónica de Tecnología Educativa*, *61*, a363. https://doi.org/10.21556/edutec.2017.61.915

Bast, S., García, P., & Montejano, G. (2017). Modelo de Datos del Sistema de Voto Electrónico Presencial OTP-Vote. *SIE, Simposio de Informática En El Estado*, 23–37.

Ben Ayed, A. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. *International Journal of Network Security & Its Applications*, *9*(3), 01–09. https://doi.org/10.5121/ijnsa.2017.9301

Caamaño, M. B., & Sabucedo, L. M. Á. (2018). *Sistema de votación mediante Blockchain*.

Cavero, S. (2014). Trabajo Final de Grado. *Sergioguillen.Com*, *710*, 1–119. http://sergioguillen.com/wp-content/uploads/2015/05/Guillen_Cavero_TFG_vFinal.pdf

De, A. (2008). *Equipo de Trabajo:* 1–8.

Del, I. (2014). *Todos somos observadores*.

Dolader, C., Bel, J., & Muñoz, J. (2017). La blockchain : fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía Industrial*, *405*, 33–40. https://dialnet.unirioja.es/servlet/articulo?codigo=6207510

Fallis, A. . (2013). 済無No Title No Title. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. (2018). Crypto-voting, a blockchain based e-voting system. *IC3K 2018 - Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, *3*(April), 223–227. https://doi.org/10.5220/0006962102230227

Goyena, R. (2019). 済無No Title No Title. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Grado, T. F. I. N. D. E. (2019). *Grado en comercio*.

Hern, R. L., Ing, C., & Navarro, D. G. (2010). *Estándares de Diseño Web*. *41*(2), 69–71.

Liu, Y., & Wang, Q. (2017). An E-voting Protocol Based on Blockchain. *IACR Cryptology EPrint Archive*, 1043.

Pesado, P., Pasini, A., Ibañez, E., Galdámez, N., Chichizola, F., Rodríguez, I., Estrebou, C., & De Giusti, A. (2008). E-Government: El voto electrónico sobre Internet. *XIV Congreso Argentino de Ciencias de La Computación*, 11.

PLAN ESTRATÉGICO 2016 - 2026. (2016).

SÁENZ, M. E. (2017). Contratos electrónicos autoejecutables y pagos con tecnología blockchain. *Revista de Estudios Europeos*, *4979*, 8. https://doi.org/10.1007/s00701-006-0874-6

Sansano Miralles, H. (2017). *Pruebas sobre sitios web*. http://rua.ua.es/dspace/handle/10045/69468

Wang, H., Zheng, Z., Xie, S., Dai, H. N., & Chen, X. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352. https://doi.org/10.1504/ijwgs.2018.10016848

2.9. ANEXOS

2.9.1. ARTÍCULO DE CIETA

ANEXO 1 ARTICULO DE CIETA

COLOMBIAN JOURNAL OF ADVANCED TECHNOLOGIES

INDICATIONS FOR PAPER SUBMITTION

Propuesta de una DAPP para un sistema de votación por internet implementando Smart contract

Ing. Cesar Yesid Barahona Rodriguez,

Estudiante de pregrado. Daniel Esteban Barreto Avila

Estudiante de pregrado. Julian Esteban Vallejo Galindo

E-mail: {cbarahona, danielebarreto, jevallejo}@ucundinamarca.edu.co

Abstract: The investigation and tecnological center (CIT) of the university Cundinamarca, has been developed a voting platform with the implementation of new technologies as Blockchain's network, for that reason it develops Smart contracts, being implemented to perfom the transactions totally secure and transparents in front of the user, since in this way it avoids possible manipulations of external people. Therefore it is consider like a decentralized network and at the same time the votes performed in the platform won't be altered.

Keywords: Blockchain, Smart contracts, Dencentralized network.

Resumen: En este documento tiene como finalidad mostrar el funcionamiento, características y aplicaciones de la red Blockchain en una votación por internet.

En la actualidad el sistema electoral tiende a tener varios déficits, tales como el error humano y la confianza de los usuarios al momento de implementar cualquier votación que permita la participación de la ciudadanía en la toma de decisiones políticas, además se dará a entender cómo funcionan los Smart contracts o más conocidos como contratos inteligentes. Ahora bien, en la actualidad Smart contracts y Blockchain es un sistema revolucionario y su estudio permitirá ver la magnitud de lo que puede aportar global y tecnológicamente al servicio de la comunidad (A. Fallís, 2013). En este caso se diseñó una plataforma de votaciones por internet para los cuerpos colegiados de la universidad de Cundinamarca siendo está una Dapp que es ciertamente la integración Blockchain con contratos inteligentes.

Palabras clave: Blockchain, votación, Smart contracts, Base de datos, transacción, Dapp.

1. **INTRODUCCIÓN**

Una Blockchain es esencialmente una base de datos distribuida en una cadena de bloques o libro de contabilidad pública de todas las transacciones o eventos digitales que se han ejecutado y compartido entre las partes participantes, cada transacción en ese libro se verifica por conceso de la mayoría de usuarios que son participantes del sistema. Una vez ingresada la información nunca puede ser borrada, la cadena de bloques contiene un registro determinado y verificable de cada transacción realizada (M. crosby, 2016).

Actualmente en Colombia se viene dando un gran debate a la reforma del código electoral, además de que nos enfrentamos a nuevos retos que se presentan por avance tecnológico en el desarrollo de las democracias (Jenny Garzon,2016).

Por consiguiente es fundamental implementar el voto por internet en Colombia y facilitar el desarrollo de las distintas formas de participación ciudadana, lo anterior tiene como consecuencia un cambio administrativo en las entidades estatales y así poder enfrentar esta nueva implementación del voto, debido a la ley 894 del 2004 estableciendo que las autoridades encargadas de las elecciones deben realizar esta implementación con el fin de estar acorde con las tendencias internacionales y mejore la democracia del país.

Por consiguiente, se está desarrollando un sistema de votaciones por internet que contiene tres partes principales: La primera parte el votante tendrá que seguir una serie de pasos para quedar registrado en el sistema ,La segunda parte del sistema abarca todo lo relacionado a la página web donde se realizará la votación y se mostraran los candidatos y sus respectivas graficas; La tercera parte abarca todo lo relacionado a la seguridad de dicho voto en la cual se implementarán Smart Contracts y la tecnología de Blockchain que aseguraran que la información del voto no se vea modificada.

La red Blockchain

En este orden de ideas la tecnología Blockchain ofrece una plataforma descentralizada, por consiguiente, envía datos de forma segura, para que el proceso de votación sea totalmente transparente y responsable con los resultados, del mismo modo las personas que participen en esto sabrán que el proceso es totalmente claro, ya que sus votos no serán alterados y su identidad no tendrá ningún riesgo(De, 2008).

Con la red Blockchain lo que se busca principalmente es un sistema de control en donde queden en segundo plano y las operaciones se puedan realizar de usuario a usuario(Fallis, 2013).

Una de las ventajas de implementar Blockchain es que proporciona de forma intrínseca tolerancia a fallos en nodos, robustez frente a manipulación y al ser pública y transparencia.

Si bien la tolerancia a fallos no es exclusiva de las cadenas de bloques, lleva el concepto a su extremo lógico al hacer que cada cuenta que comparte la base de datos valide sus cambios.

Estructura de los bloques

La blockchain almacena una gran cantidad de datos, además su tamaño es creciente con el tiempo ya que en la red sólo se añade información, por tanto, es aconsejable disponer de un mecanismo que permita la consulta eficiente como lo es un árbol de hash de merkle, que permite almacenar diversas piezas de información independiente como se puede observar en la siguiente Figura 1:

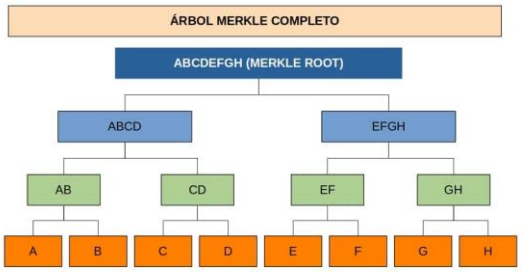


Fig. 1. Ejemplo de árbol de merkle (Dolader et al., 2017)

Propiedades fundamentales de la Blockchain

Para la creación de una blockchain se debe garantizar dos propiedades fundamentales:

1. Disponibilidad: Asegura que una transacción que ha sido emitida y verificada acabe siendo añadida a la cadena de bloques

2. Persistencia: Cuando un nodo da una transacción como estable, el resto de nodos que ya han sido verificados validen ésta como estable haciéndola inmutable

Para cumplir con la propiedad de disponibilidad, la blockchain implementa una red de nodos interconectados donde dichos nodos interaccionan como iguales (red peer-to-peer) (Bartolomé Pina et al., 2017).

Los nodos que forman parte de la red peer-to-peer disponen, cada uno de ellos, de una copia de la cadena de bloques lo cual proporciona una gran disponibilidad y robustez.

Asimismo, otra propiedad fundamental es la persistencia que se cumple cuando la cadena completa de nodos valida cada nuevo nodo antes de ser añadido y almacenado en miles de servidores lo cual hace imposible que la información que se ha verificado y almacenado sea modificada o eliminada.

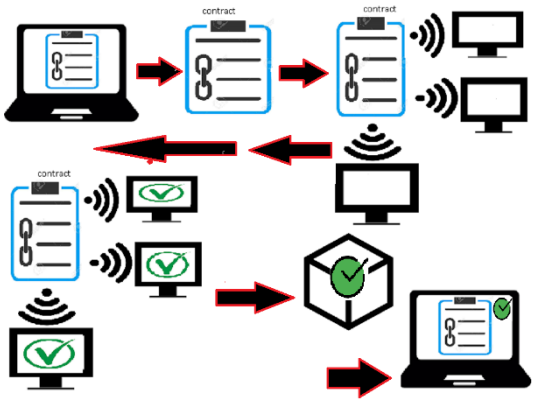


Fig. 2. Funcionamiento de la transacción en la red Blockchain, (financial times 2018).

Se puede observar en la figura 2 el funcionamiento de la blockchain, primeramente, como se agrega una transacción, después se presenta a la red como en forma de bloque, esté se transmite a todos los participantes de la red, los que están en la red aprueban que la transacción es válida, el bloque puede añadirse a la cadena proporcionando un registro transparente en las transacciones, por último, se añade la transacción a la blockchain correspondiente.

Según (Carlos Hernández, 2019) se encuentran diversos tipos de Blockchain, las cuales se explicarán a continuación

1. Blockchain públicas: Cualquier puede acceder y consultar transacciones realizadas, se permite a los usuarios hacer transacciones a la base de datos, igualmente no se pueden alterar, pero se pueden verificar, son descentralizadas ya como se mencionó anteriormente ningún usuario tiene mayor jerarquía que otro, los usuarios son rastreables debido a que la Blockchain es pública

2. Blockchain privadas: No todos los datos inscritos son públicos y únicamente los usuarios que componen la red privada pueden acceder a esta y asimismo hacer consultas y transacciones, el número de nodos que componen este tipo de red es limitado al número de usuarios, ciertamente este tipo de Blockchain nos asegura el anonimato que es requerido para cualquier realización o protección de transacciones

3. Blockchain hibridas: es la combinación de las públicas y privadas, el tipo de red de está Blockchain casi nunca están abiertas y son gestionadas por varias entidades, se usa por gobiernos y empresas que producen grandes cantidades de transacciones.

Los Smart contracts o contratos inteligentes

Se conocen como contrato electrónico y su característica principal es que son auto-ejecutables.

La ventaja de un Smart contract es que sus scripts son susceptibles de programarse en serie con sencillez al almacenarse en una cadena de bloques.

Por consiguiente, los contratos auto-ejecutables presentan ciertas ventajas ya que operan de una manera simple, rápida e inmodificable.

Algunas de las posibles funciones del Smart contract:

-Préstamos; Si el deudor no efectúa un pago, el contrato automáticamente podría revocar las

claves digitales que le dan acceso a los fondos o activar las garantías.

-Depósitos en garantía: Compras por internet; Verificada la entrega (registro del código de barras en destino, seguimiento del documento electrónico de trazabilidad, huella digital del receptor) se libera el pago.

-Controles de gasto: liberación de subvenciones y/o pagos a proyectos previa entrega de certificados.

- Herencias y donaciones: liberación de los fondos, legados etc. ante el registro del certificado de defunción (Sáenz, 2019).

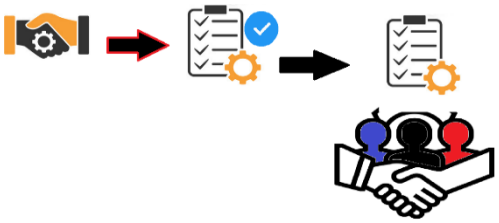


Fig 3. Funcionamiento Smart contract (Ameer Rosic, 2019).

Se puede observar en la figura 3 como es el funcionamiento del Smart contract, primeramente, las partes se ponen de acuerdo para estar en la red blockchain, seguidamente el contrato se ejecuta solo de acuerdo a los términos en el código, por último, los reguladores pueden usar la red para entender la actividad que este surgiendo.

Finalizando y por ende no menos importante se encuentra las Dapp que son parte producto final del desarrollo, Una Dapp son aplicaciones descentralizadas que utilizan 'Blockchain' para que los usuarios se relacionen directamente entre ellos y cierren acuerdos sin que exista una entidad central que gestione el control.

Plataforma web:

Es una colección de tecnologías web sobre la cual funciona un aplicativo que procesa contenido publico delimitado.

Es un sistema que sirve como base para hacer funcionar varios módulos de hardware o de software con lo que es compatible, Dicho sistema está definido por un estándar alrededor del cual se determinar una arquitectura de hardware y una plataforma de software, El principal objetivo que cumplen las plataformas digitales es facilitar la ejecución de tareas a través de programas o aplicación en un mismo lugar en la web (Hern et al., 2010).

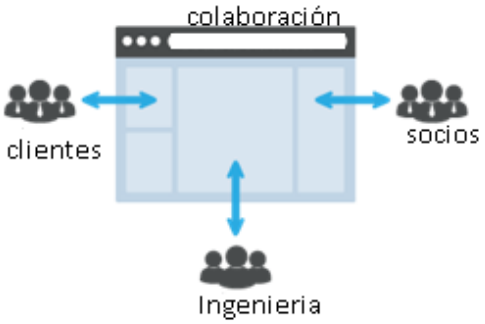


Fig..4. funcionamiento de plataforma web (Hern et al., 2010).

Se puede observar en la figura 4 como es el funcionamiento de la plataforma web, es la unión de varios colaboradores o módulos, para llevar a cabo una función en específico (Hern et al., 2010).

Los módulos que se implementaran para el correcto funcionamiento de la plataforma web son módulo de registro, módulo de la página web y el módulo encargado de la seguridad de la información del voto que utilizara la tecnología Blockchain y Smart contracts.

La plataforma web está orientada a brindar seguridad y transparencia en la votación de los cuerpos colegiados de la Universidad de Cundinamarca siendo estos la instancia que propone y apoya al consejo superior universitario y a la rectoría en temas de bienestar, al igual que reglamenta las políticas y programas creados por el Consejo superior universitario.

Para la realización de la plataforma web se utilizaron varias herramientas como muestra la figura 4 para poder llevar la plataforma a cabo:

Ganache: Ganache es una cadena de bloques personal para el desarrollo de Ethereum que puede utilizar para implementar contratos, desarrollar sus aplicaciones y ejecutar pruebas locales. Como parte de Truffle Suite, Ganache simplifica el desarrollo de las Dapp a la hora de realizar pruebas. Con Ganache, puede ver rápidamente cómo su aplicación afecta a la

cadena de bloques, y detalles introspectivos como sus cuentas, creaciones de contratos.

Web3.js: Es un conjunto de librerías que permiten la conexión con los votantes o (nodos) Ethereum por medio de un protocolo JSON-RPC y de este modo interactuar con la blockchain.

Solidity: Es un lenguaje de programación de alto nivel creado en el 2014 para aumentar el acceso a este tipo de tecnología, está basado en JavaScript y permite crear contratos inteligentes de una forma más amigable con el programador.

Truffle: Es un entorno de desarrollo que facilita la integración de contratos inteligente en la cadena de bloques, convirtiendo lenguaje de programación como solidity a binario que es el formato que acepta la blockchain.

MetaMask: MetaMask es la forma más fácil de interactuar con las DApps en un navegador. Es una extensión para Chrome o Firefox que se conecta a una red Ethereum sin ejecutar un nodo completo en la máquina. Puede conectarse a la red principal de Ethereum y a cualquier red de prueba, en este caso se conectara a Ganache (Grado, 2019) .

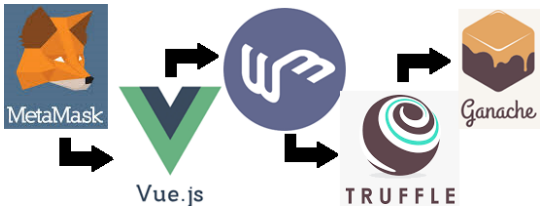


Fig. 4. Como se implementa el voto por medio de Blockchain (Sáenz, 2019).

Conclusiones

La blockchain permite implementar una base de datos distribuida, pública e inmutable basada en una secuencia creciente de bloques. Esta base de datos tiene muchas ventajas, una de las más importantes es la tolerancia a fallos en nodos, robustez frente a manipulación y al ser pública, transparencia para asegurar que la información del voto no sea alterada de ninguna forma y al implementar Smart Contracts generar un contrato autoejecutable que opere de una manera simple, rápida e inmodificable.

Los contratos inteligentes son un programa informático que ejecuta un acuerdo entre dos partes y se basan en la tecnología Blockchain permitiendo automatizar gran cantidad de procesos de forma segura y así garantizar la confidencialidad e integridad del voto.

Estas tecnologías están demostrando su importancia en el futuro ya que están revolucionando todo tipo de acuerdos sustituyendo la valoración humana por sistemas neutros rápidos y eficientes, prescindiendo así de intermediarios ahorrando costos y disminuyendo el fraude electoral.

Referencias

Acosta, I., Nieto, E., & Barahona, C. (2015). Metodología para la evaluación de calidad de los productos software de la Universidad de Cundinamarca. *ENGI Revista Electrónica de La Facultad de Ingeniería*, *3*(2), 4. http://webcache.googleusercontent.com/search?q=cache:hPdc3fbYpooJ:revistas_electronicas.unicundi.edu.co/index.php/Revistas_electronicas/article/download/157/152+&cd=2&hl=en&ct=clnk&gl=co

Bartolomé Pina, A. R., Bellver Torlà, C., Castañeda Quintero, L., & Adell Segura, J. (2017). Blockchain en Educación: introducción y crítica al estado de la cuestión. *Edutec. Revista Electrónica de Tecnología Educativa*, *61*, a363. https://doi.org/10.21556/edutec.2017.61.915

Bast, S., García, P., & Montejano, G. (2017). Modelo de Datos del Sistema de Voto Electrónico Presencial OTP-Vote. *SIE, Simposio de Informática En El Estado*, 23–37.

Ben Ayed, A. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. *International Journal of Network Security & Its Applications*, *9*(3), 01–09. https://doi.org/10.5121/ijnsa.2017.9301

Caamaño, M. B., & Sabucedo, L. M. Á. (2018). *Sistema de votación mediante Blockchain*.

Cavero, S. (2014). Trabajo Final de Grado. *Sergioguillen.Com*, *710*, 1–119. http://sergioguillen.com/wp-content/uploads/2015/05/Guillen_Cavero_TFG_vFinal.pdf

De, A. (2008). *Equipo de Trabajo:* 1–8.

Del, I. (2014). *Todos somos observadores*.

Dolader, C., Bel, J., & Muñoz, J. (2017). La

blockchain : fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía Industrial*, *405*, 33–40. https://dialnet.unirioja.es/servlet/articulo?codigo=6207510

Fallis, A. . (2013). 済無No Title No Title. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. (2018). Crypto-voting, a blockchain based e-voting system. *IC3K 2018 - Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, *3*(April), 223–227. https://doi.org/10.5220/0006962102230227

Goyena, R. (2019). 済無No Title No Title. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Grado, T. F. I. N. D. E. (2019). *Grado en comercio*.

Hern, R. L., Ing, C., & Navarro, D. G. (2010). *Estándares de Diseño Web*. *41*(2), 69–71.

Liu, Y., & Wang, Q. (2017). An E-voting Protocol Based on Blockchain. *IACR Cryptology EPrint Archive*, 1043.

Pesado, P., Pasini, A., Ibañez, E., Galdámez, N., Chichizola, F., Rodríguez, I., Estrebou, C., & De Giusti, A. (2008). E-Government: El voto electrónico sobre Internet. *XIV Congreso Argentino de Ciencias de La Computación*, 11.

PLAN ESTRATÉGICO 2016 - 2026. (2016).

SÁENZ, M. E. (2017). Contratos electrónicos autoejecutables y pagos con tecnología blockchain. *Revista de Estudios Europeos*, *4979*, 8. https://doi.org/10.1007/s00701-006-0874-6

Sansano Miralles, H. (2017). *Pruebas sobre sitios web*. http://rua.ua.es/dspace/handle/10045/69468

Wang, H., Zheng, Z., Xie, S., Dai, H. N., & Chen, X. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352. https://doi.org/10.1504/ijwgs.2018.10016848

2.9.2. ARTÍCULO DE CICI

ANEXO 2 ARTICULO DE CICI

MÓDULO BLOCKCHAIN, PRUEBAS DE CARGA Y ESTRÉS

Daniel Esteban Barreto Avila [1][0000-0002-3292-4174], Julian Esteban Vallejo Galindo [2][0000-0002-4006-1575], Cesar Yesid Barahona Rodriguez [3][0000-0001-7673-7381] and Gina Maribel Valenzuela Sabogal[4][0000-0002-2833-1579]

[1] Universidad de Cundinamarca, Colombia
[2] Universidad de Cundinamarca, Colombia
[3] Universidad de Cundinamarca, Colombia
[4] Universidad de Cundinamarca, Colombia
danielebarreto@ucundinamarca.edu.co
jevallejo@ucundinamarca.edu.co
cbarahona@ucundinamarca.edu.co
gvalenzuela@ucundinamarca.edu.co

Resumen: Este documento tiene como objetivo principal, mostrar las pruebas de carga y estrés al momento de realizar las votaciones realizadas a través de la dapp que se está implementando en la universidad de Cundinamarca para los cuerpos colegiados de la misma. una dapp no es más que la unión de los Smart contract o contratos inteligentes y la red blockchain a través de internet, ahora bien, las pruebas de software generan la posibilidad de identificar y eliminar los defectos que surgen dentro del proceso de un sistema productivo o llevado a producción para brindar soluciones informáticas con buenos estándares de calidad que cumplan con los requisitos funcionales de la aplicación.
Palabras claves: Dapp, Smart contract, Blockchain, votación, pruebas

Abstract. The main objective of this document is to show the burden and effort test at the moment of carrying out the voting carried out through the Dapp that is being implemented at the University of Cundinamarca for the collegiate bodies of the same, Una Dapp is nothing more that the union of smart contracts or smart contracts and the blockchain network through the internet, now the software tests generate the possibility of identifying and eliminating the defects that arise within the process of a productive or led system In production, however, testing of software products focuses on providing computer solutions with good quality standards that meet the functional requirements of the application.
Keywords: Dapp, Smart contract, Blockchain, voting, test

Introducción

La red Blockchain se creó para manejar el historial de transacciones del bitcoin además de ofrecer una base de datos inmutable; dicho de otra manera, una base de datos que no puede ser alterada o modificada, basada en una secuencia de bloques, estos al ser públicos generan una confianza en base a la transparencia y la solidez de la misma, ciertamente todo lo que se encuentra en la red siempre va a tener una brecha de seguridad, es decir que hasta el momento la red Blockchain no ha sido hackeada (Dolader et al., 2017).

Igualmente, la tecnología Blockchain ofrece una plataforma descentralizada, es decir que permite a los usuarios enviar datos de forma segura, para que el proceso de votación sea totalmente transparente y responsable con los resultados, del mismo modo las personas que participen en esto sabrán que el proceso es totalmente claro, ya que sus votos no serán alterados y su identidad no tendrá ningún riesgo(De, 2008).

Ahora bien, la universidad de Cundinamarca se centra en los proyectos orientados a la web los cuales deben ser diseñados y orientados con estándares internacionales de calidad. Por esta razón se diseña desde el modelado del software hasta las pruebas funcionales, la metodología para la calidad del software está compuesta de dos partes; la primera enfocada en la documentación y modelación de los proyectos y la segunda dirigida a las pruebas de testeo entre estas las de carga y estrés para determinar lo rápido que un sistema realiza una tarea en unas determinadas condiciones de trabajo (Acosta et al., 2015).

Escenarios de prueba

Para hacer más óptimo el proceso de carga y estrés se usó software libre, los cuales nos ayudan a sistematizar todo el desarrollo de las pruebas funcionales del software, se pueden evaluar todos los tipos de petición este caso como se puede ver en la tabla 1:

Tabla 1. Peticiones HTTP

Petición	Función
Get	Solicita información o recurso al servidor
Post	Envía información al servidor para que este la procese
Delete	Envía la petición de eliminar el recurso especificado
Put	Envía un recurso al servidor

Fuente: (Sansano Miralles, 2017).

Para facilitar el proceso de evaluación de calidad se cuenta con el uso de herramientas libres las cuales sistematizan el proceso dado; en este caso:

- **JMeter:** Es un software de código abierto diseñada en java para cargar el comportamiento funcional del software, realizando las pruebas por carga y estrés, así mismo medir el rendimiento y tiempo de las mismas.

Resultados

Se realizó la prueba de carga y estrés al proyecto de voto electrónico por internet para los cuerpos colegiados de la universidad de Cundinamarca, módulo blockchain, usando una cantidad específica de usuarios como se puede demostrar a continuación, además de esto se verifico que cada usuario pudiese votar sin que se ocupara el servidor, esto funciono debido a que la red blockchain implementa transacciones continuas y seguras.

Para dichas pruebas de rendimiento se implementó una de las herramientas más populares la cual es JMeter (open source), esta herramienta cuenta con numerosos componentes que pueden constar en una realización de pruebas, uno de los más importantes es el componente (Thread Group) que representa un grupo específico de usuarios con los que se desea realizar las pruebas; Además de este componente existen los Controllers (Sampler, Logic Controller), los Samplers son los que realizan peticiones contra la aplicación y los Logic Controllers establecen el orden en que se ejecutan dichas peticiones.

Por consiguiente, se especifica el puerto en las configuraciones 'HTTP(S) Test Script Recorder' que en este caso es el 8181 después de configurar el puerto se debe configurar el proxy del navegador con el puerto que se especificó anteriormente y la dirección IP del equipo en el que se vayan a realizar las pruebas, una vez configurado el puerto, el proxy, la cantidad de usuarios y las peticiones que se realizaran a la aplicación se procede a configurar los componentes con los cuales se obtendrán los resultados al momento de realizar las pruebas los cuales son los (Listeners) que son los que recopilan los datos de las peticiones que realizan los Samplers y el (Timer) con el cual se puede añadir tiempo extra a la ejecución de las peticiones que se realizan contra la aplicación y obtener el tiempo que se demora al momento de realizar las pruebas con la cantidad de usuario que se especificó en el Thread Group; Una vez completado las configuraciones en JMeter se proceden a realizar las peticiones haciendo click en el botón 'Run'.

Entonces se procede a realizar las pruebas de rendimiento con la cantidad de usuarios (1, 10, 100, 1.000, 10.000, 100.000, 1’000.000 y 100’000.000) y se obtuvieron los siguientes resultados como se observa en la Figura 1.

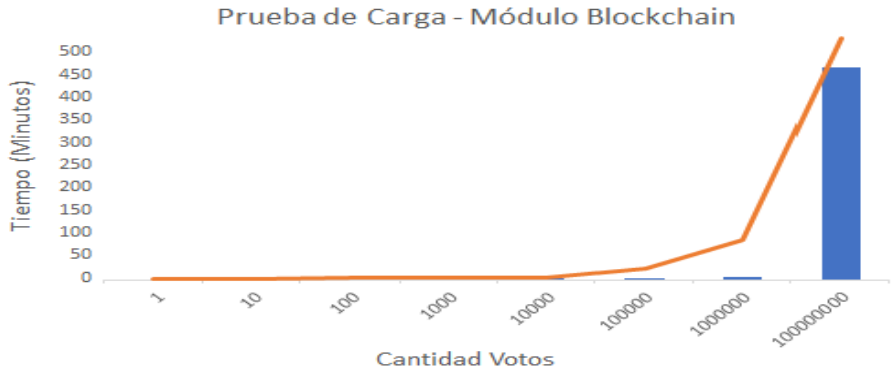


Fig 1. Prueba de carga Cantidad de usuarios vs Tiempo de respuesta

Los detalles de las pruebas de carga y estrés realizadas se pueden observar en la Tabla 2.

Tabla 2. Detalles Cantidad de usuarios vs Tiempo (minutos)

Cantidad de usuarios	1	10	100	1.000	10.000	100.000	1’000.000	100’000.000
Tiempo	1	2	3	4	5	21	79	476

Conclusiones

Al momento de realizar la prueba de carga los tiempos de respuesta son bastante óptimos debido a que con cien millones de transacciones no se superaron los cuatrocientos setenta y seis (476) minutos equivalentes a 7 horas para completar las respectivas votaciones de los 100.0000.000 de usuarios lo cual hace que los tiempos sean demasiado pequeños comparado con la gran cantidad de votaciones con las que se hicieron las pruebas.

Además, la prueba de estrés que se implementó, se demostró que la aplicación puede soportar más de (100’000.000) de usuarios y seguir funcionando correctamente no se rompió o genero algún tipo de fallos con esta prueba se demuestra la solidez de la aplicación en los momentos de carga extrema o con demasiados usuarios realizando sus respectivas votaciones; Esta prueba también permitió determinar que la aplicación desarrollada rendirá lo suficiente en caso de que la cantidad de usuarios realizando sus votaciones supere a la cantidad de usuarios esperados.

Así mismo, la prueba de carga realizada al módulo blockchain con una cantidad escalable de usuarios desde cien (100) hasta cien millones de usuarios (100’000.000) demostraron que el sistema cumple con los criterios de rendimiento para realizar votaciones en los cuerpos colegiados de la Universidad de Cundinamarca.

Por consiguiente, se ha implementado un sistema de votación por internet capaz de ser probado en producción y soportar los diferentes procesos electorales de los cuerpos colegiados que la universidad de Cundinamarca, superando así las pruebas de carga y estrés realizadas el módulo blockchain.

Referencias

Acosta, I., Nieto, E., & Barahona, C. (2015). Metodología para la evaluación de calidad de los productos software de la Universidad de Cundinamarca. *ENGI Revista Electrónica de La Facultad de Ingeniería*, *3*(2), 4. http://webcache.googleusercontent.com/search?q=cache:hPdc3fbYpooJ:revistas_electronicas.unicundi.edu.co/index.php/Revistas_electronicas/article/download/157/152+&cd=2&hl=en&ct=clnk&gl=co

Bartolomé Pina, A. R., Bellver Torlà, C., Castañeda Quintero, L., & Adell Segura, J. (2017). Blockchain en Educación: introducción y crítica al estado de la cuestión. *Edutec. Revista Electrónica de Tecnología Educativa*, *61*, a363. https://doi.org/10.21556/edutec.2017.61.915

Bast, S., García, P., & Montejano, G. (2017). Modelo de Datos del Sistema de Voto Electrónico Presencial OTP-Vote. *SIE, Simposio de Informática En El Estado*, 23–37.

Ben Ayed, A. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. *International Journal of Network Security & Its Applications*, *9*(3), 01–09. https://doi.org/10.5121/ijnsa.2017.9301

Caamaño, M. B., & Sabucedo, L. M. Á. (2018). *Sistema de votación mediante Blockchain*.

Cavero, S. (2014). Trabajo Final de Grado. *Sergioguillen.Com*, *710*, 1–119. http://sergioguillen.com/wp-content/uploads/2015/05/Guillen_Cavero_TFG_vFinal.pdf

De, A. (2008). *Equipo de Trabajo:* 1–8.

Del, I. (2014). *Todos somos observadores*.

Dolader, C., Bel, J., & Muñoz, J. (2017). La blockchain : fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía Industrial*, *405*, 33–40. https://dialnet.unirioja.es/servlet/articulo?codigo=6207510

Fallis, A. . (2013). 済無No Title No Title. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. (2018). Crypto-voting, a blockchain based e-voting system. *IC3K 2018 - Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, *3*(April), 223–227. https://doi.org/10.5220/0006962102230227

Goyena, R. (2019). 済無No Title No Title. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Grado, T. F. I. N. D. E. (2019). *Grado en comercio*.

Hern, R. L., Ing, C., & Navarro, D. G. (2010). *Estándares de Diseño Web*. *41*(2), 69–71.

Liu, Y., & Wang, Q. (2017). An E-voting Protocol Based on Blockchain. *IACR Cryptology EPrint Archive*, 1043.

Pesado, P., Pasini, A., Ibañez, E., Galdámez, N., Chichizola, F., Rodríguez, I., Estrebou, C., & De Giusti, A. (2008). E-Government: El voto electrónico sobre Internet. *XIV Congreso Argentino de Ciencias de La Computación*, 11.

PLAN ESTRATÉGICO 2016 - 2026. (2016).

SÁENZ, M. E. (2017). Contratos electrónicos autoejecutables y pagos con tecnología blockchain. *Revista de Estudios Europeos*, *4979*, 8. https://doi.org/10.1007/s00701-006-0874-6

Sansano Miralles, H. (2017). *Pruebas sobre sitios web*. http://rua.ua.es/dspace/handle/10045/69468

Wang, H., Zheng, Z., Xie, S., Dai, H. N., & Chen, X. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352. https://doi.org/10.1504/ijwgs.2018.10016848

2.9.3. MANUAL DE USUARIO

ANEXO 3 MANUAL DE USUARIO

UDEC
UNIVERSIDAD DE CUNDINAMARCA

SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO BLOCKCHAIN

MANUAL DE USUARIO

DESARROLLO DE SOFTWARE
UNIVERSIDAD DE CUNDINAMARCA

Institución de educación superior sujeta a inspección y vigilancia por el Ministerio de Educación Nacional

www.unicundi.edu.co
unicundi@mail.unicundi.edu.co
Línea gratuita 018000 976000

Dirección de Sistemas y Tecnología
sistemasytecnologia@mail.unicundi.edu.co
PBX: 828 14 83 Ext. 110-170
Sede Fusagasugá

TABLA DE CONTENIDO

LISTA DE FIGURAS

INTRODUCCIÓN

El módulo blockchain, hace parte del proyecto sistema de voto electrónico para los Cuerpos Colegiados de la universidad de Cundinamarca, con el fin de obtener una votación segura y confiable.

Lo que se logro es establecer un voto simple, seguro e invulnerable a ataques realizados(hacking) para beneficiar a algún tercero, se han realizado servicios web para hacer comunicación con la parte front-end que hace parte del mismo proyecto ya mencionado anteriormente.

1. USUARIO GENERAL

Los usuarios que utilicen nuestra (API) será el módulo front-end del proyecto “SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO PLATAFORMA WEB”, este módulo contara con una interfaz gráfica basada en la comunicación mediante servicios REST con la red blockchain y sus correspondientes Smart contracts o contratos inteligentes.

2. REQUISITOS DE SOFTWARE

Hardware

Computador de escritorio o portátil con navegador web que soporte HTML5 y JavaScript, con espacio disponible en disco duro y memoria RAM mínimo 4GB

Software

- Sistema operativo Windows 7 en adelante
- Truffle versión 5.1.42
- Solidity 0.5.16
- Node v.12.18.4
- Web3js v1.21
- Ganache

3. APLICATIVO (API)

A continuación, se describen de manera más detallada las funciones realizadas en la API, para poder tener un voto fiable y seguro.

3.1 COMPILAR LOS SMART CONTRACTS (API)

Una vez realizado el Smart contract para la votación, se procede a compilar el contrato como se puede ver en la siguiente imágen, se usarán los comandos:

truffle compile

truffle migrate --reset

Primeramente, para compilar los contratos debe tener abierta la aplicación de Ganache Truffle.

```
C:\Users\ISAACELEAZAR\Desktop>cd Documentación proyecto de grado\api\api\blockchain

C:\Users\ISAACELEAZAR\Desktop\Documentación proyecto de grado\api\api\blockchain>truffle compile

Compiling your contracts...
===========================
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\Voting.sol
> Artifacts written to C:\Users\ISAACELEAZAR\Desktop\Documentación proyecto de grado\api\api\contracts
> Compiled successfully using:
   - solc: 0.5.16+commit.9c3226ce.Emscripten.clang


C:\Users\ISAACELEAZAR\Desktop\Documentación proyecto de grado\api\api\blockchain>truffle migrate --reset

Compiling your contracts...
===========================
> Compiling .\contracts\Migrations.sol
```

Figura 32. Compilado de Smart contract

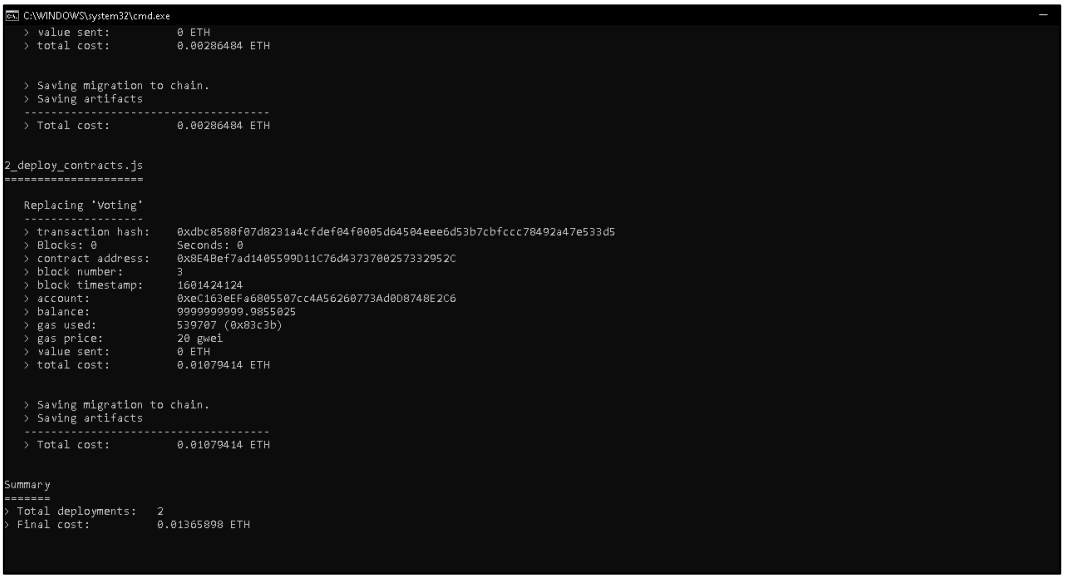


Figura 33 Contratos compilados y migrados

3.2. COMPILAR ENTORNO DE DESARROLLO DE LOS SERVICIOS WEB

Una vez migrado los Smart contract se procede a compilar el entorno de desarrollo con el comando: “**npm run dev”**, como se puede ver en la siguiente en la siguiente imágen, el servicio ya quedara levantado y listo para ser consumido.

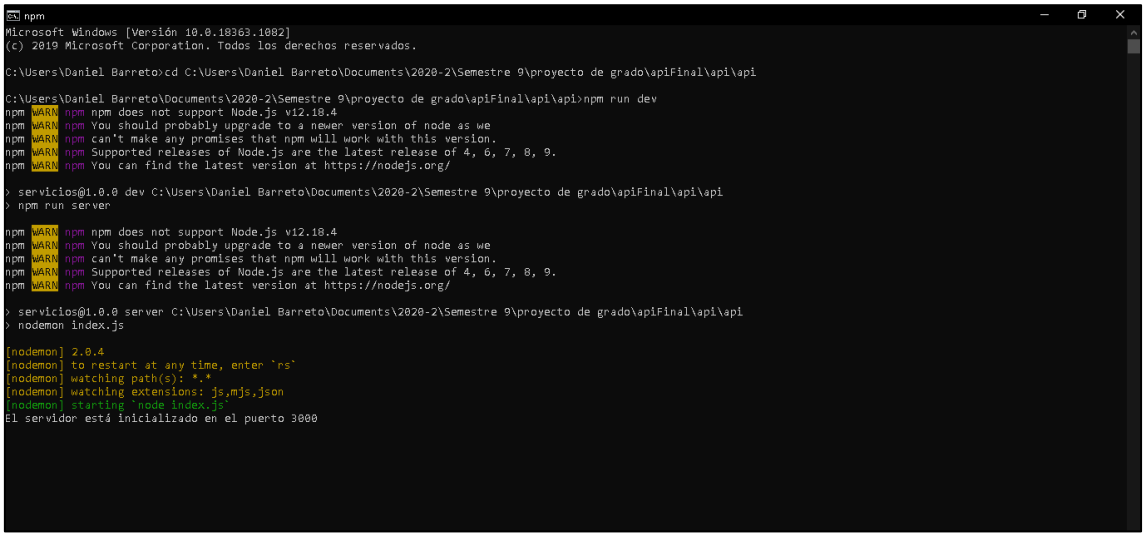


Figura 34 Entorno de desarrollo

3.3 PRUEBAS CON POSTMAN

Ahora bien, para probar que los servicios estén funcionando y optimizados para ser consumidos se usó el software Postman que nos permite crear peticiones y enviarlas al servidor que escucha en este caso el puerto 3000, gracias a este software libre nos dimos cuenta que el API ya se encontraba listo para ser usado por el módulo front-end

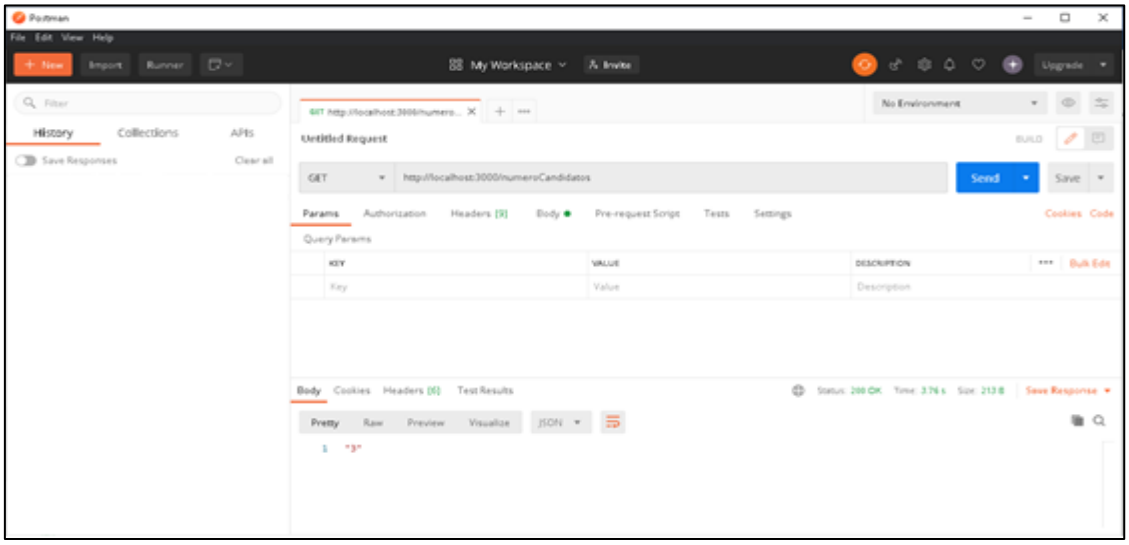


Figura 35 Prueba de número de candidatos

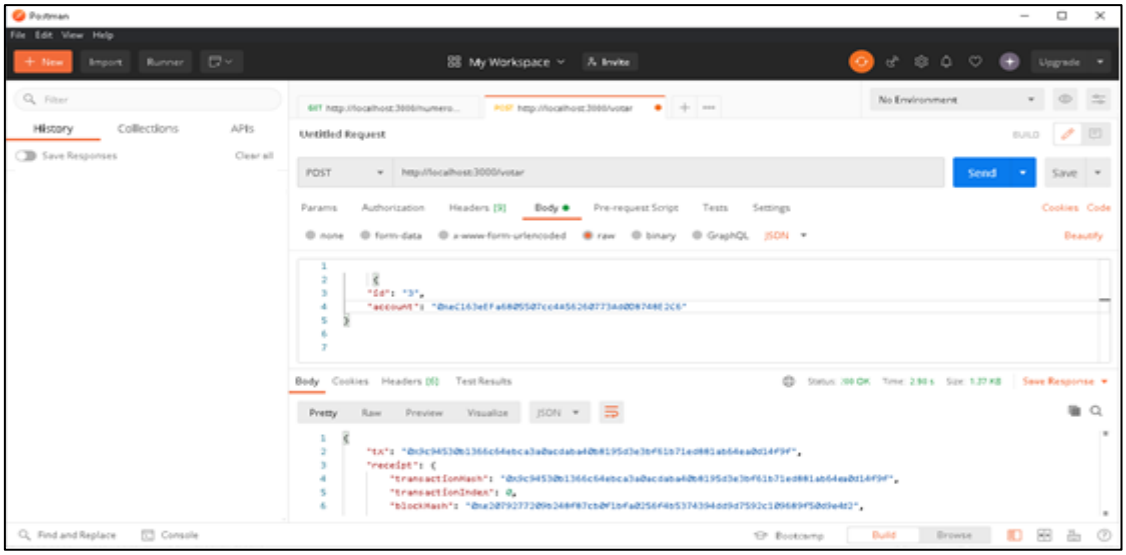


Figura 36. Prueba de votar

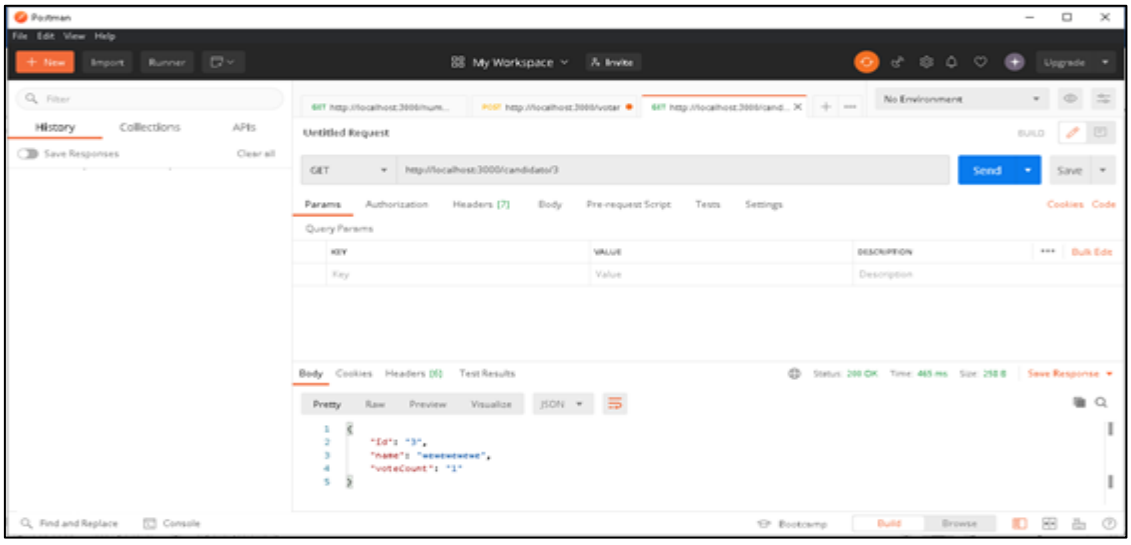


Figura 37 Prueba de traer el voto

2.9.4. MANUAL DE INSTALACIÓN

ANEXO 4 MANUAL DE INSTALACIÓN

UDEC
UNIVERSIDAD DE CUNDINAMARCA

SISTEMA DE VOTO ELECTRÓNICO PARA LOS CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA, MÓDULO BLOCKCHAIN

MANUAL DE INSTALACIÓN DESARROLLO DE SOFTWARE UNIVERSIDAD DE CUNDINAMARCA

Institución de educación superior sujeta a inspección y vigilancia por el Ministerio de Educación Nacional

www.unicundi.edu.co
unicundi@mail.unicundi.edu.co
Línea gratuita 018000 976000

Dirección de Sistemas y Tecnología
sistemasytecnologia@mail.unicundi.edu.co
PBX: 828 14 83 Ext. 110-170
Sede Fusagasugá

TABLA DE CONTENIDO

LISTA DE FIGURAS

Manual de instalación

El presente manual de instalación está dirigido al personal técnico responsable de la instalación y configuración del Sistema de voto electrónico para los Cuerpos Colegiados de la universidad de Cundinamarca, Módulo Blockchain, en este se especifican las herramientas necesarias para el despliegue del aplicativo.

1.Requisitos mínimos

El módulo está diseñado para funcionar en un sistema con los requisitos mínimos presentados a continuación, esto permitirá que el dispositivo soporte las herramientas necesarias para un correcto despliegue y rendimiento.

1.1. Hardware

Almacenamiento en disco duro disponible: 2,0 GB

Processador mínimo: Core

Memória RAM: 4GB

1.2. Software

Sistema operativo Windows 8 en adelante

2. INSTALACION DE PROGRAMAS

Se aclara que los enlaces de instalación y sus imágenes relacionadas pueden variar a lo largo del tiempo.

2.1. Ganache | Truffle Suite

Ganache es una herramienta que nos permitirá ejecutar una blockchain en local, donde podremos desplegar nuestros Smart contracts, ejecutar test e inspeccionar de un modo visual el estado de la blockchain mientras hacemos nuestras operaciones.

2.1.2. Ganache | Truffle Suite, descarga

Para la descarga se accede al enlace que presentará la opción de descarga y se pulsa el botón **Download**.

Enlace: https://www.trufflesuite.com/ganache

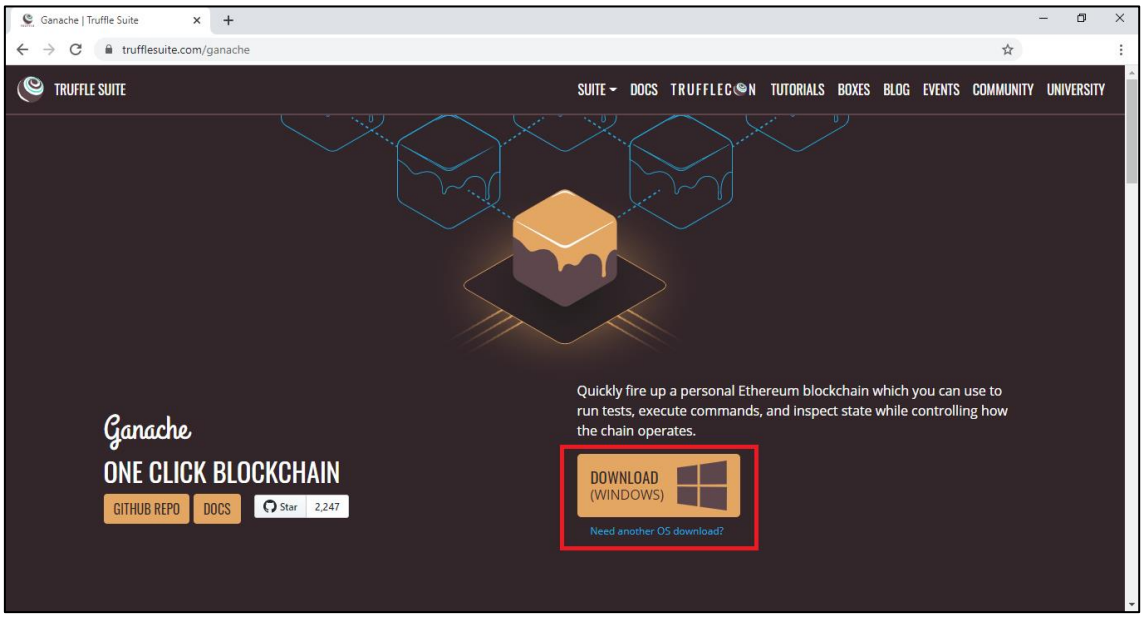


Figura 38 Ganache, enlace de descarga

2.1.3. Ganache | Truffle Suite, instalación

Una vez completada la descarga se procede a instalar ganache, para continuar pulsar el botón **instalar.**

Figura 39 Ganache, instalación

2.1.4. Ganache | Truffle Suite, iniciar

Una vez terminada la instalación se procede a pulsar el botón **Inicio Rápido (QUICKSTART).**

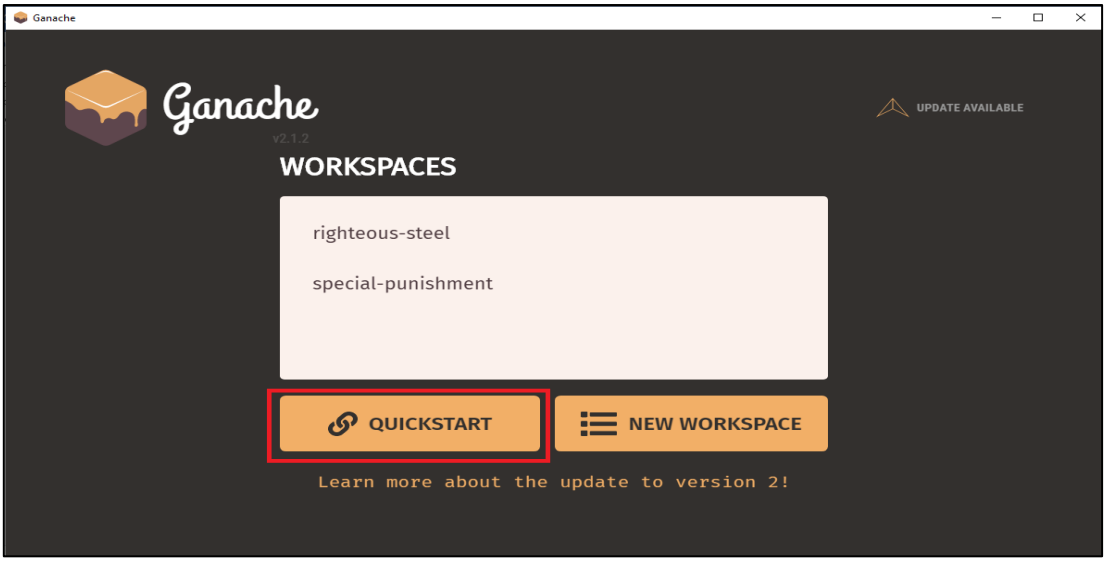


Figura 40 Ganache, iniciar

2.1.5. Ganache | Truffle Suite, instalación terminada

Una vez completados los pasos se visualiza la siguiente interfaz verificando que la herramienta Ganache quedó correctamente instalada.

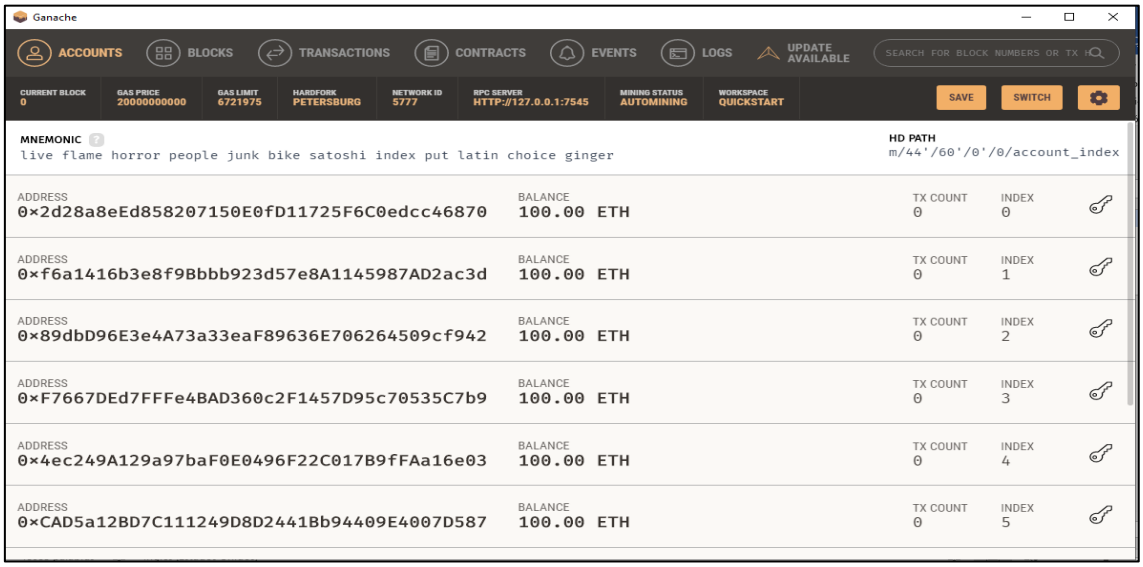


Figura 41 Ganache, instalación terminada

2.2. Postman

Postman es una herramienta que principalmente nos permite crear peticiones y enviar peticiones http a servicios REST mediante una interface gráfica de una forma muy sencilla y poder, de esta manera, probar las APIs.

2.2.1. Postman, descarga

Para la descarga se accede al enlace que presentará la opción de descarga y se pulsa el botón **Download the app**.

Enlace: https://www.postman.com/downloads/

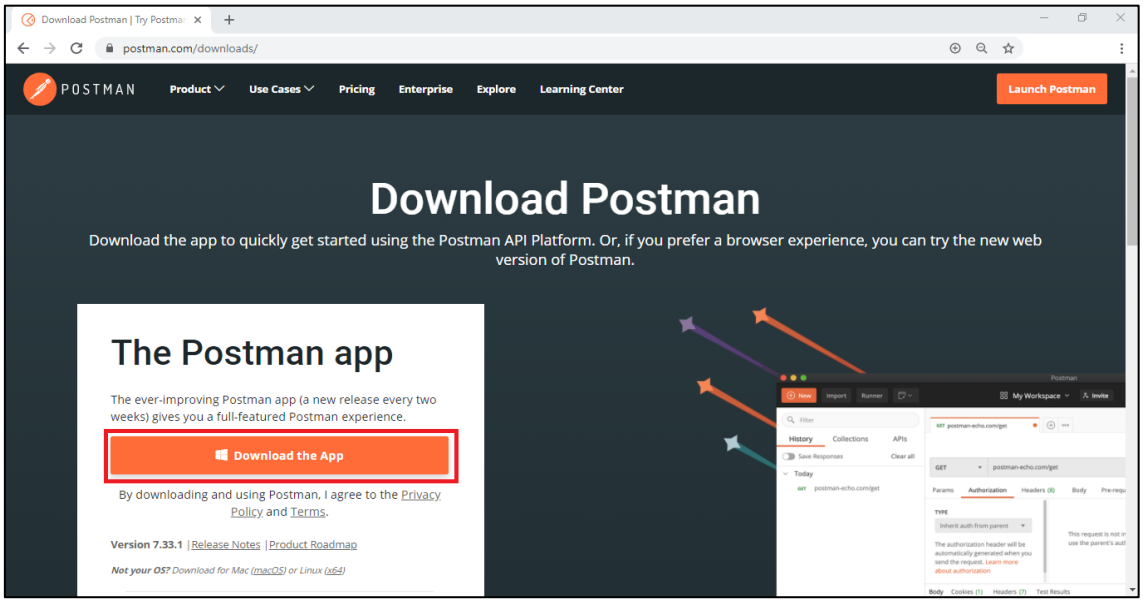


Figura 42 Postman, enlace de descarga

2.2.2. Postman, seleccionar versión de Windows

Una vez pulsado el botón de descarga se presenta la opción de descarga tanto para las versiones de Windows 32bits como para 64bits.

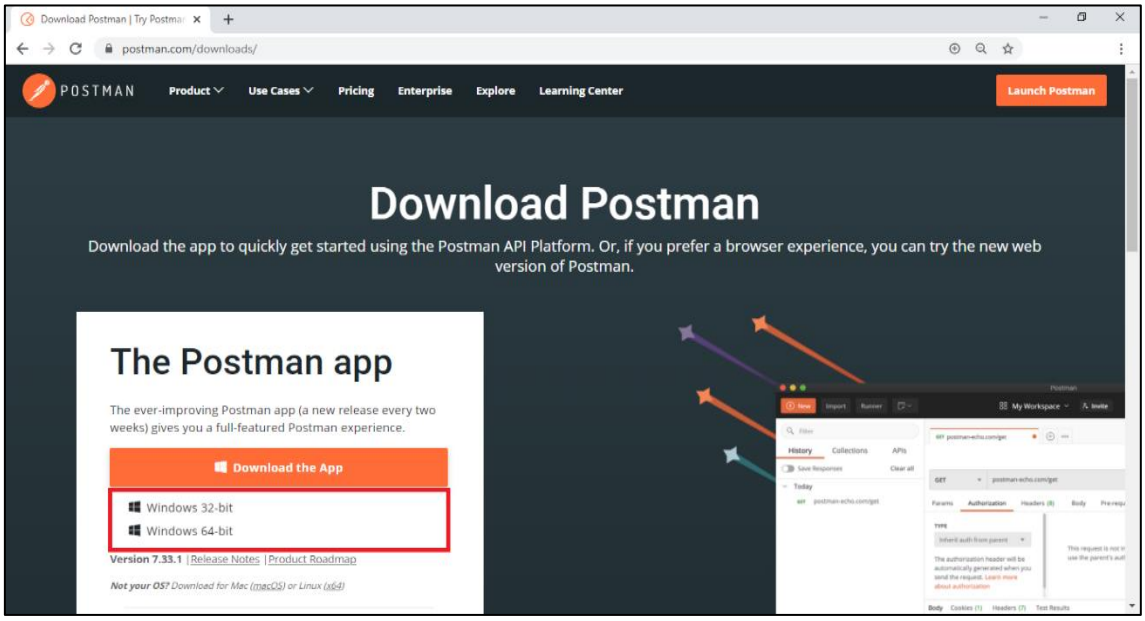


Figura 43 Postman, enlace de descarga versions Windows

2.2.3. Postman, instalación

Una vez descargado el archivo .exe se procede a darle doble click para instalarlo.

Figura 44 Postman, instalación

2.2.4. Postman, iniciar

Una vez completados los pasos se visualiza la siguiente interfaz verificando que la herramienta Postman quedó correctamente instalada.

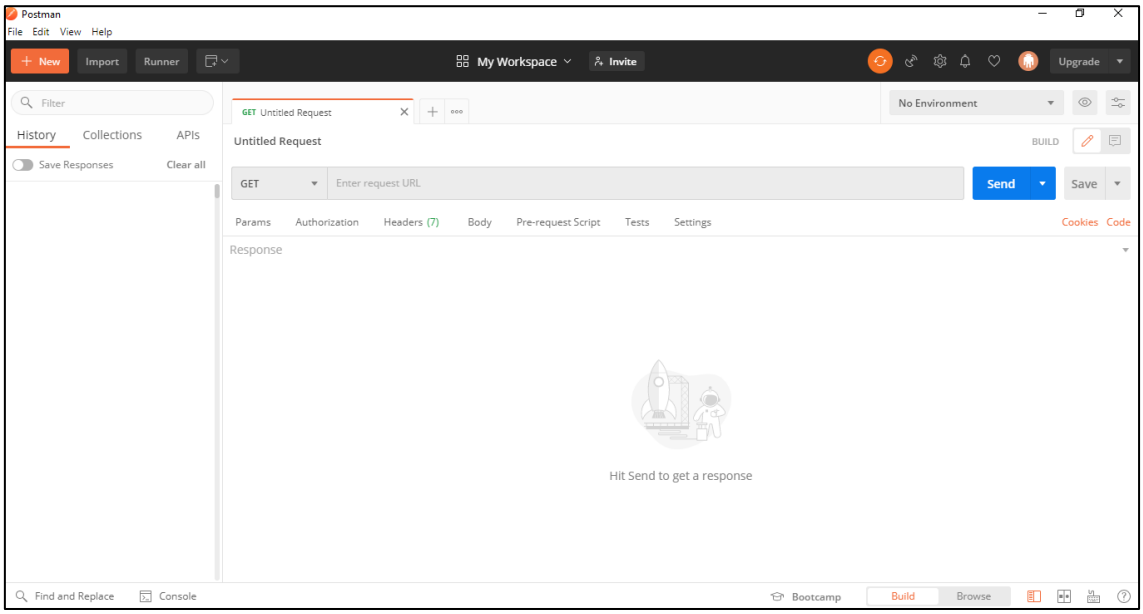


Figura 45 Postman, instalación terminada

2.3. Node.JS

Node.js es un entorno en tiempo de ejecución multiplataforma, de código abierto, para la capa del servidor basado en el lenguaje de programación JavaScript, asíncrono, con E/S de datos en una arquitectura orientada a eventos.

2.3.1. Node.JS, descarga

Para la descarga se accede al enlace que presentara dos opciones, versión LTS que es la recomendada y la versión actual que podría presentar errores que aún no han sido detectados.

Enlace: https://nodejs.org/es/download/

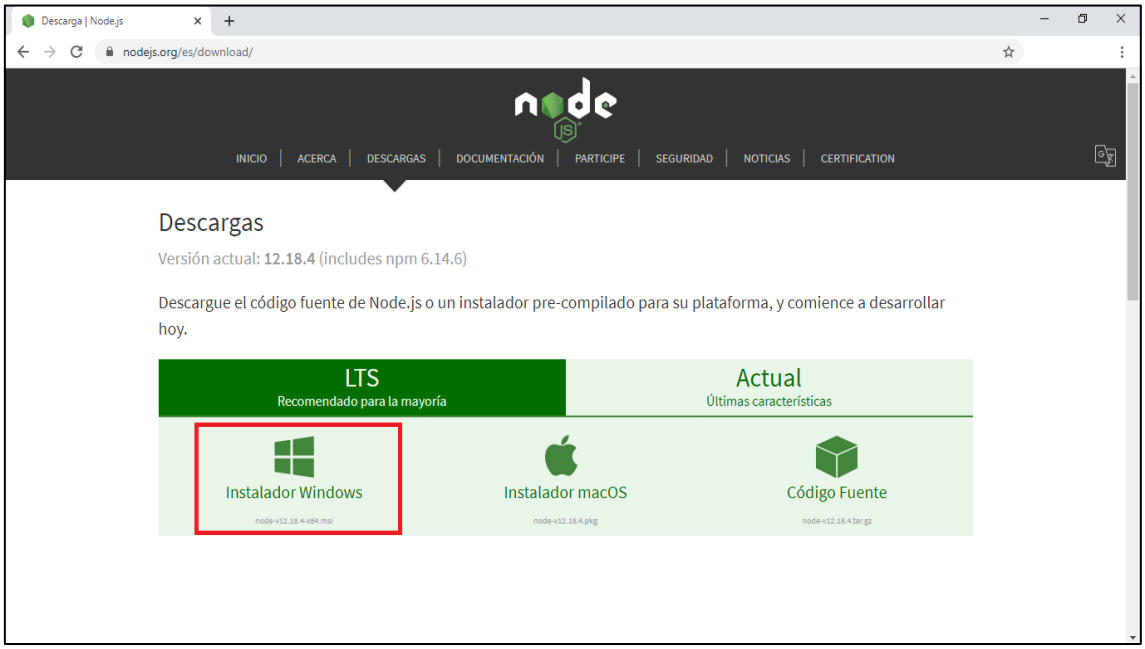


Figura 46 Node.JS, descarga

2.3.2. Node.JS, instalación

Una vez descargado se ejecuta el .exe y se procede a la instalación, pulsar el botón **Siguiente.**

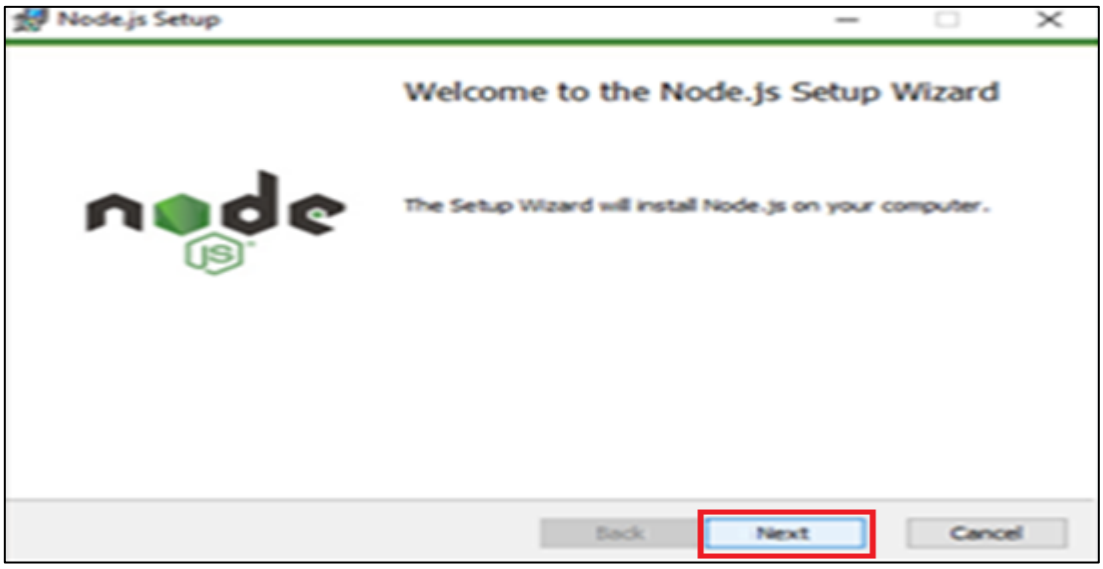


Figura 47 Node.JS, inicio instalación

Se muestran los términos de licencia, pulsar en la casilla para aceptar los términos y pulsar el botón **Siguiente**.

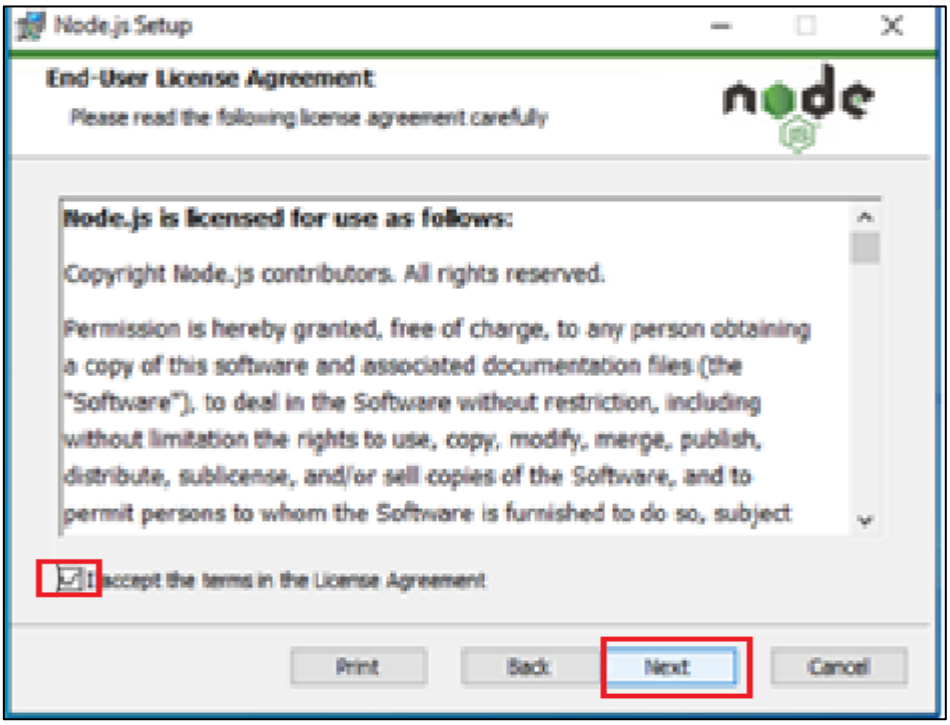


Figura 48 Node.JS, Ventana términos y condiciones

A continuación, pulsar el botón **Siguiente** continuar.

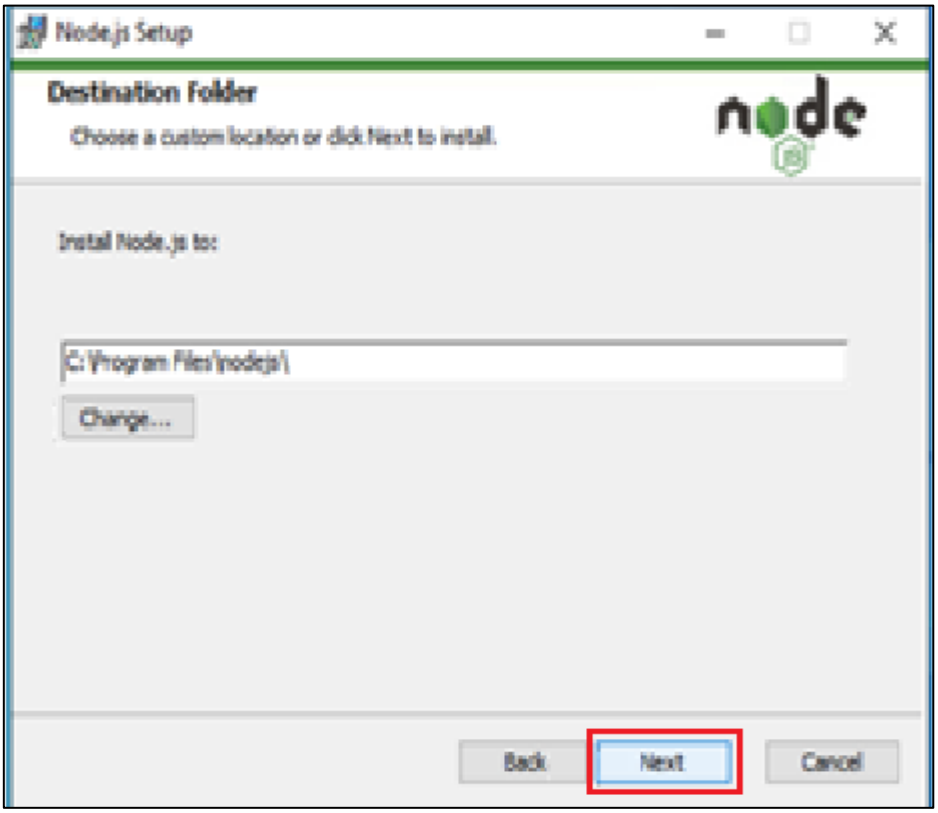


Figura 49 Node.JS, ubicación

Se muestran los diferentes paquetes que ofrece Node.JS, en este caso todos son necesarios, pulsar el botón Siguiente para continuar.

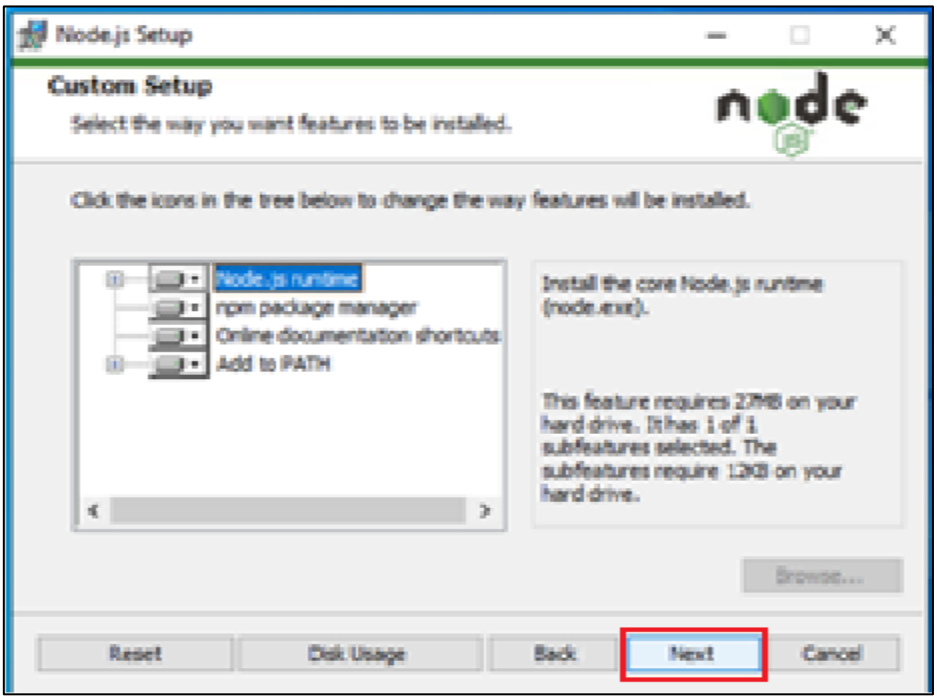


Figura 50 Node.JS, paquetes

Para finalizar pulsar el botón instalar para comenzar la instalación, los permisos de administrador son necesarios.

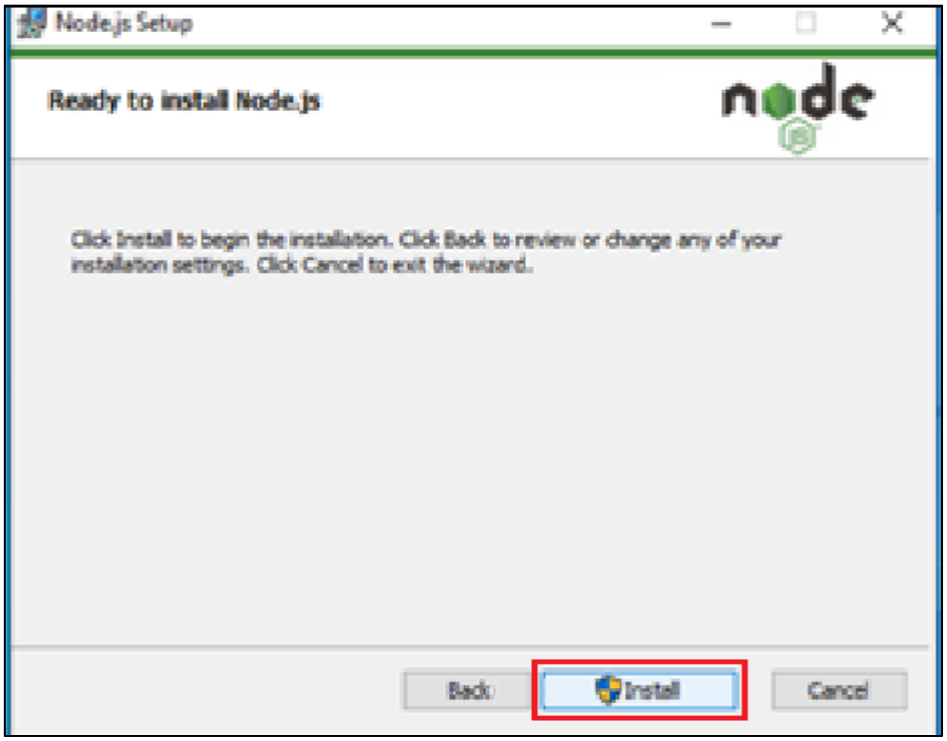


Figura 51 Node.JS, instalación

Una vez finalizada la instalación se procede a verificar que haya sido correcta, a través de la ventana de comandos (CMD) se ejecuta la instrucción “**node -v**”, si la instalación fue exitosa la ventana mostrará la versión instalada.

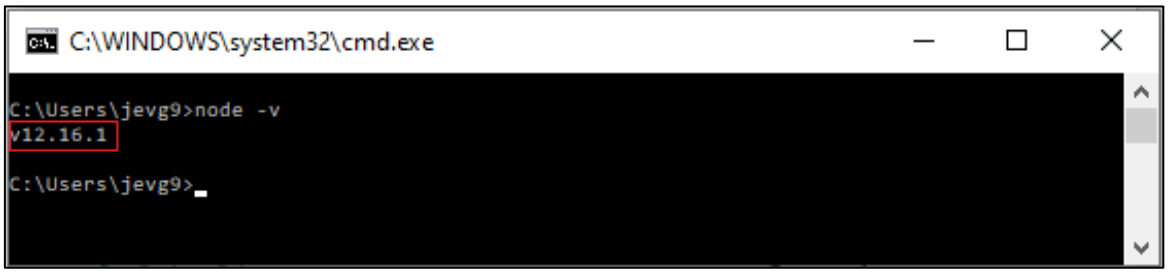


Figura 52 Node.JS, verificar versión instalada

2.4. Web3.JS

Es una API en JavaScript compatible con Ethereum que implementa las especificaciones genéricas en formato JSON.

2.4.1. Web3.JS, instalación

Para instalar Web3.js se necesita escribir el siguiente comando en la ventana de comandos (CMD) "**npm install web3**"

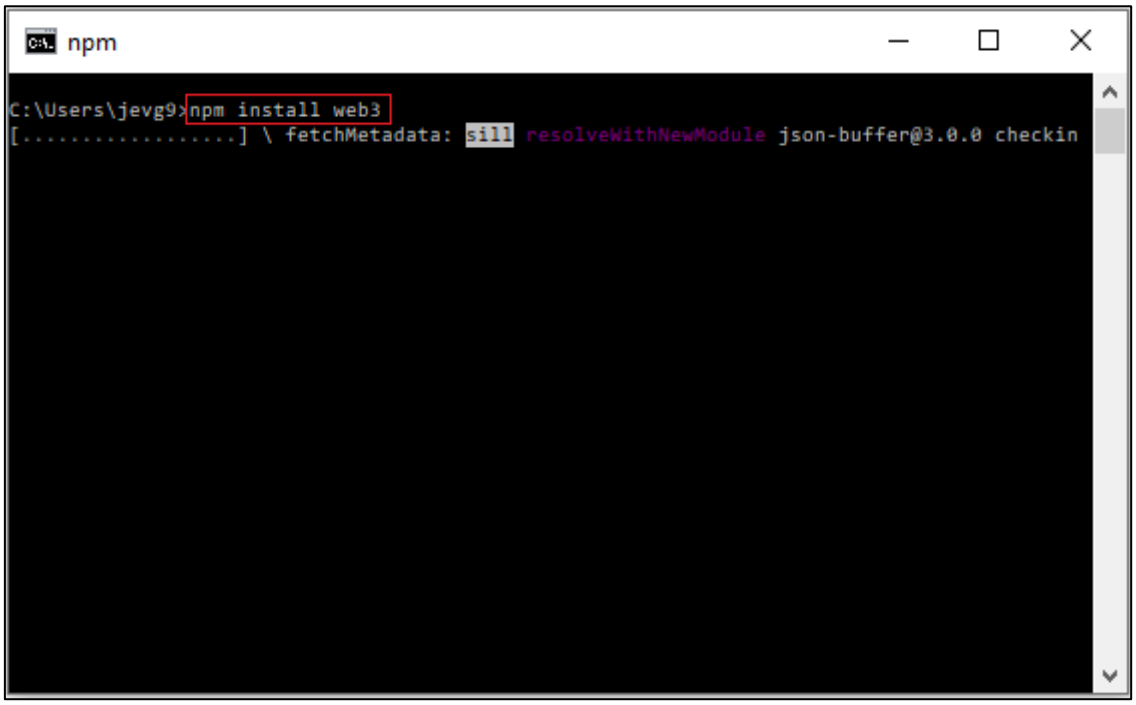


Figura 53 Web3.JS, instalación

2.5. Solidity

Solidity es un lenguaje de programación orientado a objetos para escribir contratos inteligentes. Se utiliza para implementar contratos inteligentes en varias plataformas blockchain, en particular, Ethereum.

2.5.1. Solidity, instalación

Para instalar Solidity se necesita escribir el siguiente comando en la ventana de comandos (CMD) "**npm install -g solc**"

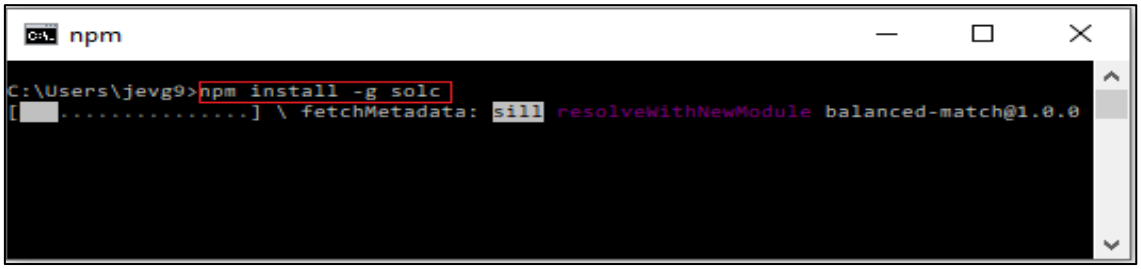


Figura 54 Solidity, instalación

2.6. Truffle

El marco Truffle es una herramienta para construir, probar, implementar y automatizar el flujo de trabajo para DApps basados en blockchain de Ethereum.

2.6.1. Truffle, instalación

Para instalar Truffle se necesita escribir el siguiente comando en la ventana de comandos (CMD) "**npm install -g truffle**"

Figura 55 Truffle, instalación

Una vez finalizada la instalación de truffle se procede a verificar que haya sido correcta, a través de la ventana de comandos (CMD) se ejecuta la instrucción "**truffle version**", si la instalación fue exitosa la ventana mostrará la versión instalada.

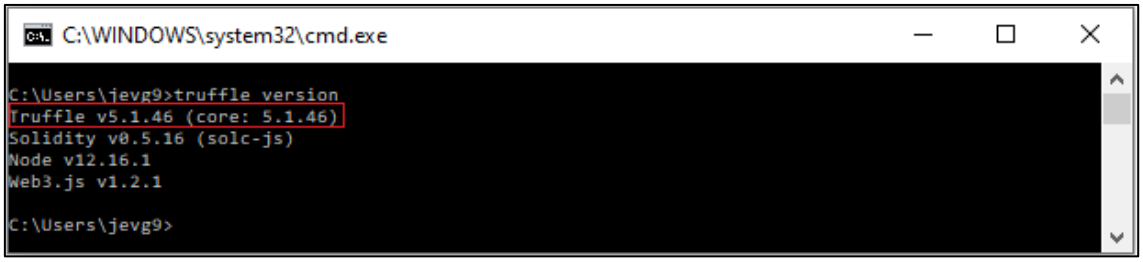


Figura 56 Truffle, verificar versión instalada

2.9.5. DISEÑO DE LA RED BLOCKCHAIN IMPLEMENTANDO UN CONTRATO INTELIGENTE

ANEXO 5 DISEÑO CONTRATO INTELIGENTE

Para el modelo propuesto en este proyecto del Sistema de voto electrónico para los Cuerpos Colegiados de la universidad de Cundinamarca en el que se implementa una red Blockchain, así como de los Smart Contracts o contratos inteligentes los cuales se integrarán ya que en los Smart Contracts se va a establecer las reglas de las votaciones.

- BLOCKCHAIN ETHEREUM

Ethereum soporta Contratos Inteligentes ya que fue la primer blockchain que introdujo el concepto de “Smart Contracts” pues es mediante estos contratos que se establecerán las reglas para realizar la votación.

Además, utiliza como algoritmo de consenso PoW (Proof of Work) para recompensar a los mineros que puedan añadir nuevos bloques y como mecanismo de defensa de un posible ataque DoS (Denegation of Service), esto hace más seguras las transacciones, pero también las hace más lentas por el costo computacional que implica adicionar un bloque a la cadena. Es este coste computacional el que hace que no sea rentable un ataque.

Para la implementación del proyecto del Sistema de voto electrónico para los Cuerpos Colegiados de la universidad de Cundinamarca, Módulo Blockchain se implementa la red Blockchain Ethereum.

Figura 57 Ethereum, Blockchain

- DISEÑO DE SMART CONTRACTS IMPLEMENTADOS EN LA RED BLOCKCHAIN

Como se menciona anteriormente un Smart Contract es un acuerdo cuya ejecución es automatizable y ejecutable. Automatizable por computadora, aunque algunas partes pueden requerir entrada y control humano. Ejecutable por la ejecución legal de los derechos y obligaciones o la ejecución a prueba de falsificaciones. Es una pieza de código ejecutable, para Ethereum el código puede ser C, C++, Go, JavaScript, Python, Java y Solidity.

El lenguaje utilizado en este proyecto de Sistema de voto electrónico para los Cuerpos Colegiados de la universidad de Cundinamarca, Módulo Blockchain es Solidity.

Para el desarrollo del modelo propuesto se usan Smart Contracts. Estos Smart Contracts se basan en los Contratos Legales en los que se establecería una votación y su seguridad.

En este contrato de votaciones se deben incluir las reglas o funciones en las que se desarrollará la votación que para este proyecto serán las siguientes:

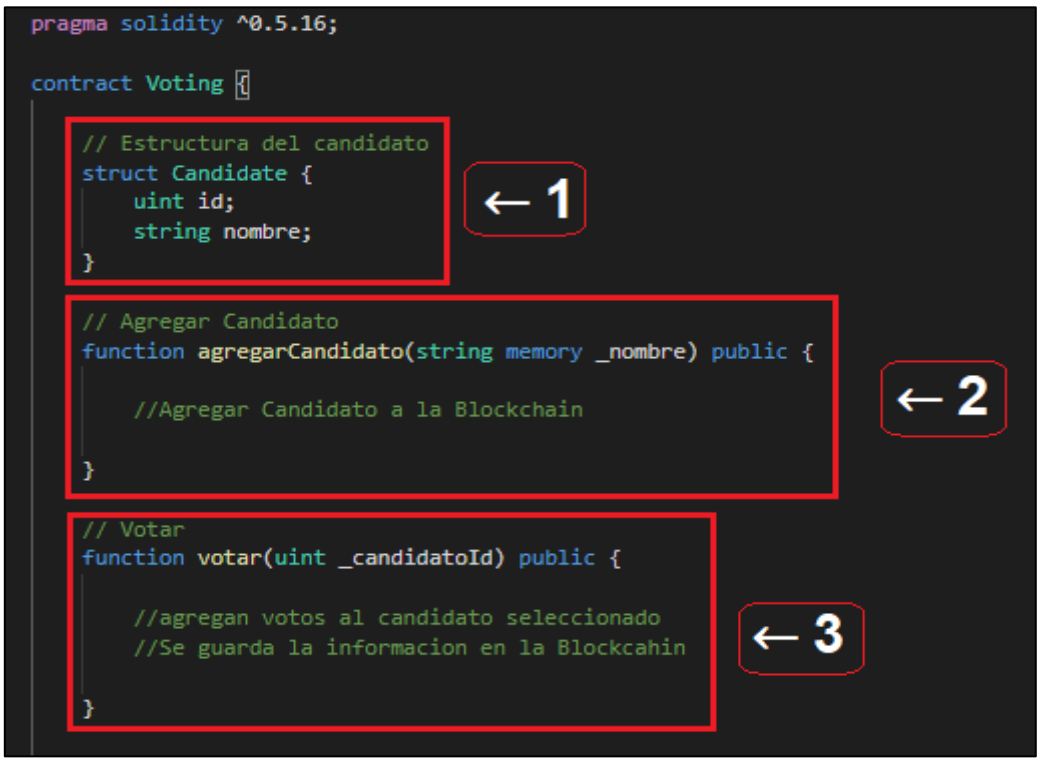


Figura 58 Estructura Smart Contract de votación

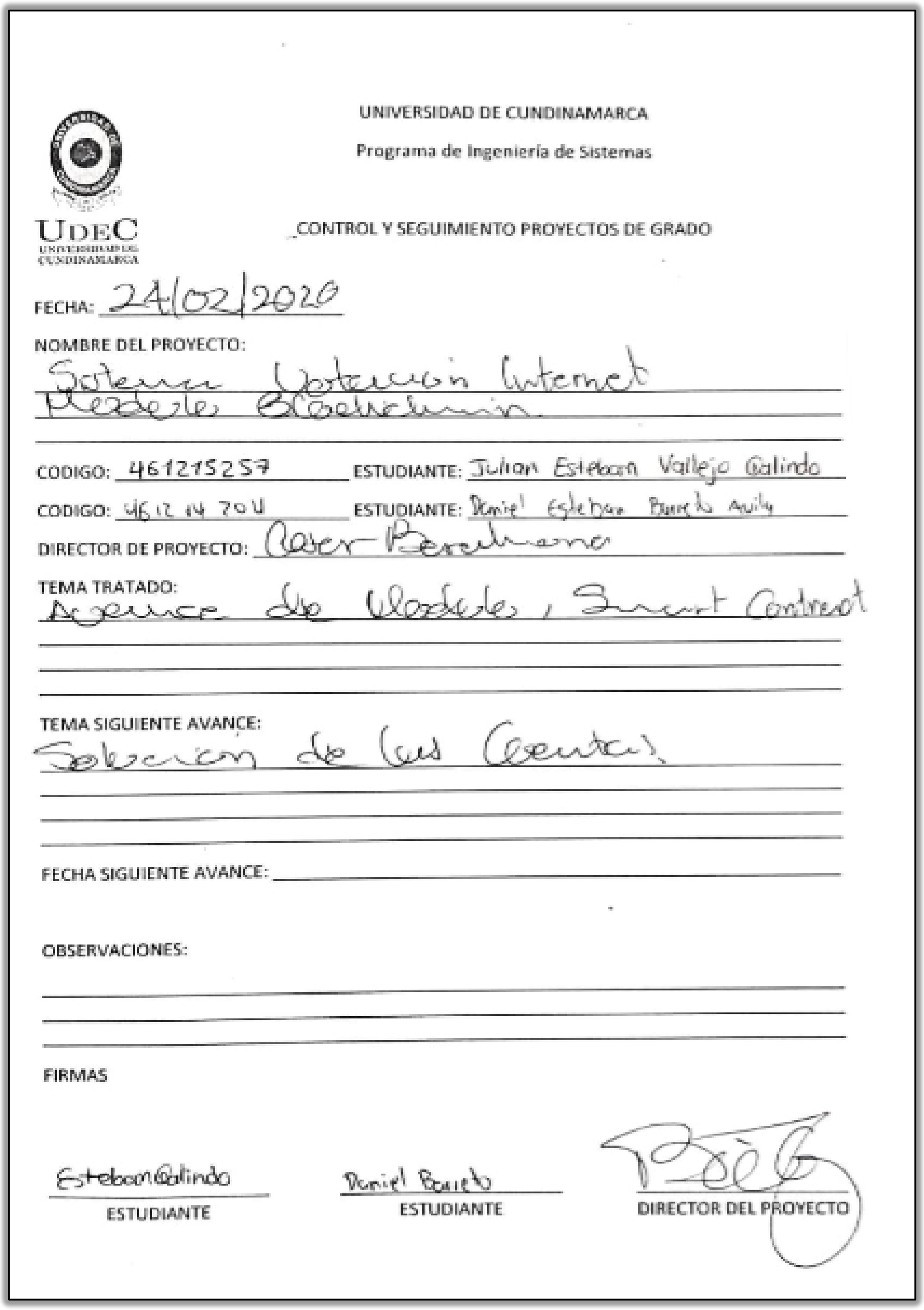
1. Estructura del Candidato: Se tendrá la estructura del candidato como su nombre con su respectivo identificador.
2. Agregar Candidato: Para el diseño del Smart Contract es necesario incluir la opción de Agregar un Candidato para que posteriormente se pueda votar por dicho candidato, para agregar un candidato es necesario un nombre al cual se le asignara un identificador único.

3. Votar: La función principal del Smart Contract es votar es aquí donde se enviará la información del voto a la red Blockchain para posteriormente hacer el conteo de los votos recibidos por ese candidato.

   Es importante aclarar que una vez iniciada la votación si se requiere hacer alguna modificación en los Smart Contracts esta no se verá reflejada ya que cada vez que se necesita hacer algún cambio se debe iniciar la votación otra vez, esto como medida de seguridad para que no hayan alteraciones en medio de la votación iniciada, debido a que una vez iniciada la votación el Smart Contract (figura 48) se añade a la Blockchain la cual no permite cambios en los Smart Contracts.

2.9.6. FORMATOS DE SEGUIMIENTO

ANEXO 6 FORMATOS DE SEGUIMIENTO



UNIVERSIDAD DE CUNDINAMARCA

Programa de Ingeniería de Sistemas

UDEC UNIVERSIDAD DE CUNDINAMARCA

CONTROL Y SEGUIMIENTO PROYECTOS DE GRADO

FECHA: 24/02/2020

NOMBRE DEL PROYECTO: Sistema Votación Internet Mediante Blockchain

CODIGO: 461215257 ESTUDIANTE: Julian Esteban Vallejo Galindo

CODIGO: 461214704 ESTUDIANTE: Daniel Esteban Barreto Avila

DIRECTOR DE PROYECTO: Cesar Berdugo

TEMA TRATADO: Avance de Modelos, Smart Contract

TEMA SIGUIENTE AVANCE: Selección de las Cuentas

FECHA SIGUIENTE AVANCE:

OBSERVACIONES:

FIRMAS

Esteban Galindo — ESTUDIANTE

Daniel Barreto — ESTUDIANTE

DIRECTOR DEL PROYECTO

Figura 59 Seguimiento 24 Febrero de 2020

UNIVERSIDAD DE CUNDINAMARCA

Programa de Ingeniería de Sistemas

UDEC
UNIVERSIDAD DE CUNDINAMARCA

CONTROL Y SEGUIMIENTO PROYECTOS DE GRADO

FECHA: 03/03/2020

NOMBRE DEL PROYECTO:
Sistema Votación por Internet modulo blockchain.

CODIGO: 461215257 ESTUDIANTE: Julian Esteban Vallejo Galindo

CODIGO: 461214704 ESTUDIANTE: Daniel Esteban Barreto Avila

DIRECTOR DE PROYECTO: Cesar Yesid Barahona R.

TEMA TRATADO:
Revisión Articulo, modificar titulo Figuras, explicación sistema.

TEMA SIGUIENTE AVANCE:
Correcciones finales del Articulo.

FECHA SIGUIENTE AVANCE:

OBSERVACIONES:
No se hizo seleccionado lo de Ganache

FIRMAS

Esteban Galindo
ESTUDIANTE

Daniel Barreto
ESTUDIANTE

DIRECTOR DEL PROYECTO

Figura 60 Seguimiento 03 Marzo de 2020

SEGUIMIENTOS REUNIONES VIRTUALES

Las siguientes imágenes son evidencias de las reuniones realizadas de manera virtual por medio de la aplicación Microsoft Teams.

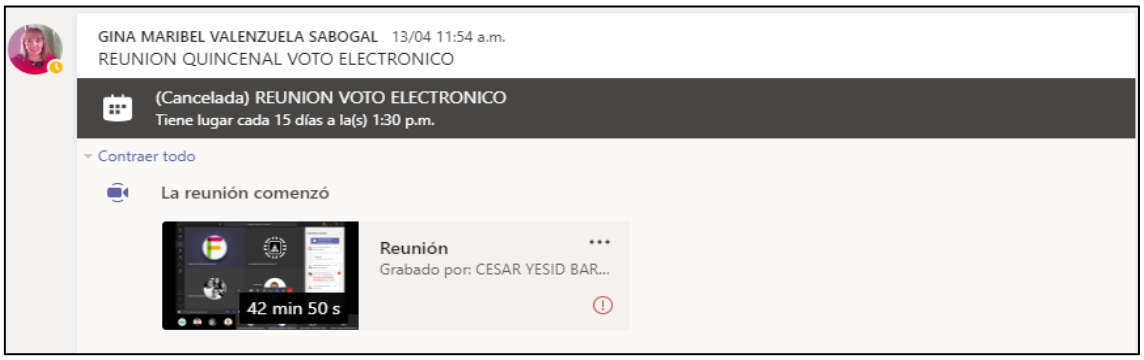


Figura 61 Seguimiento Microsoft Teams 13 Mayo de 2020

Figura 62 Seguimiento Microsoft Teams 08 Junio de 2020

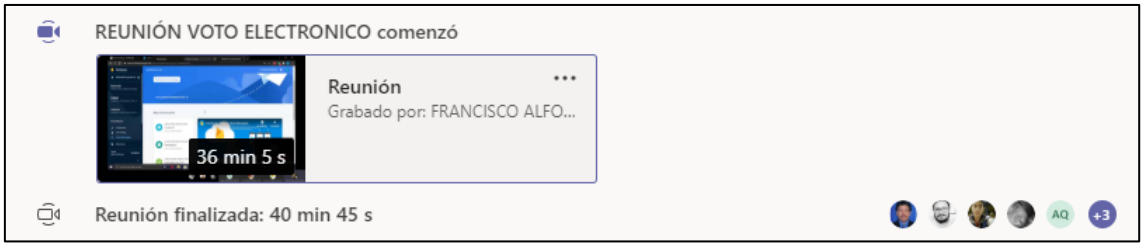


Figura 63 Seguimiento Microsoft Teams 17 Junio de 2020

Figura 64 Seguimiento Microsoft Teams 15 Julio de 2020

Figura 65 Seguimiento Microsoft Teams 29 Julio de 2020

Figura 66 Seguimiento Microsoft Teams 12 Agosto de 2020

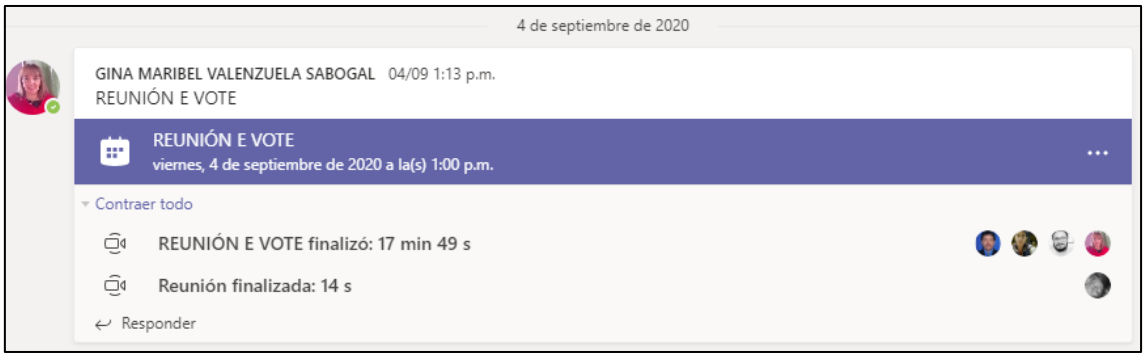


Figura 67 Seguimiento Microsoft Teams 04 Septiembre de 2020

Figura 68 Seguimiento Microsoft Teams 16 Octubre de 2020

Figura 69 Seguimiento Microsoft Teams 23 Octubre de 2020

Figura 70 Seguimiento Microsoft Teams 30 Octubre de 2020