ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Desarrollo de una Aplicación Descentralizada de voto electrónico para comicios académicos

PROYECTO INTEGRADOR

Previo la obtención del Título de:

Ingeniero en Telemática

Presentado por:

Rommel Patricio Saquicela Loja

Omar Geovanny Ordoñez Valle

GUAYAQUIL - ECUADOR

Año: 2021

DECLARACIÓN EXPRESA

”Los derechos de titularidad y explotación, nos corresponde conforme al reglamento de propiedad intelectual de la institución; Rommel Saquicela, Omar Ordoñez damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual”

Rommel Saquicela

Omar Ordoñez

EVALUADORES

Jose Cordova
PROFESOR DE LA MATERIA

Washington Velázquez
PROFESOR TUTOR

RESUMEN

En la actualidad la ESPOL maneja un sistema de votación electrónico presencial y centralizado, donde los votantes tienen que estar físicamente en el recinto electoral para emitir su voto y la entidad gubernamental es la que controla el conteo y la emisión de resultados. Este sistema de votación tradicional no ha estado exento de quejas por parte de los votantes y las agrupaciones políticas. Los votantes indican que tienen que soportar largas colas para sufragar y las agrupaciones políticas manifiestan tener desconfianza en la entidad electoral que administra los comicios, al no existir un seguimiento de la elección en tiempo real. La meta de este proyecto es diseñar un sistema de votación remoto y descentralizado en el cual el votante pueda emitir su voto desde su teléfono inteligente, y la administración de la elección no tenga que ser controlada por una autoridad central. La herramienta tecnológica que se utilizó para desarrollar este sistema de votación fue Flutter. Este kit de desarrollo permitió crear la aplicación web para la entidad electoral y la aplicación móvil para el usuario. Blockchain con su esquema de red Ethereum surgió como mecanismo propicio para agregar seguridad al sistema de votación propuesto. Como conclusión tenemos una aplicación web en el que la entidad electoral despliega una elección sin la necesidad de imprimir papeletas de votación. Además el votante cuenta con una aplicación móvil en la que puede ejercer su derecho al voto, para que no necesite acudir físicamente al recinto electoral.

Palabras Clave: Blockchain, Descentralizado, Ethereum, Flutter, Voto electrónico,

ABSTRACT

ESPOL currently operates a centralized, face-to-face electronic voting system, where voters have to be physically in the polling place to cast their vote and the government entity is the one that controls the counting and issuance of results. This traditional voting system has not been without complaints from voters and political groups. Voters indicate that they have to endure long lines to vote and political groups express mistrust in the electoral entity that administers the elections, as there is no real-time monitoring of the election. The goal of this project is to design a decentralized remote voting system in which the voter can cast their vote from their smartphone, and the administration of the election does not have to be controlled by a central authority. The technological tool that was used to develop this voting system was Flutter. This development kit allowed us to create the web application for the electoral entity and the mobile application for the user. Blockchain with its Ethereum network scheme emerged as a suitable mechanism to add security to the proposed voting system. As a conclusion we have a web application in which the electoral entity displays an election without the need to print ballot papers. In addition, the voter has a mobile application in which he exercises his right to vote, so that he does not need to physically go to the polling place.

Keywords: Blockchain, Decentralized, Electronic vote, Ethereum, Flutter

ÍNDICE GENERAL

ABREVIATURAS

ESPOL	Escuela Superior Politécnica del Litoral
DB	Base de datos
ETH	Ethereum

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

1. INTRODUCCIÓN

La Escuela Superior Politécnica del Litoral (ESPOL) desde hace muchos años tiene adoptada una forma de gobierno democrática, donde los estudiantes, personal docente y administrativo, eligen a sus autoridades mediante mecanismos electorales. Las facultades de este centro universitario implementan este modelo de sufragio de acuerdo a sus propias realidades. El cambio de un sistema convencional electrónico a voto electrónico con Blockchain es una decisión difícil de tomar debido a que los actores electorales deben recibir una preparación exhaustiva para manejar este nuevo sistema de votación[1].

Los procesos electorales han evolucionado con los últimos avances de las Tecnologías de la Información y Comunicación (TICs) [1]. La seguridad en las redes de datos permite protección, integridad y veracidad de la información. La diversidad de propuestas para resguardar información ha logrado significativos avances tecnológicos en cuanto a mantener los datos protegidos y fuera del alcance de terceros. Uno de los métodos más seguros para realizar transacciones en redes de datos es la herramienta llamada Blockchain. Esta herramienta permite intercambiar información de forma segura sin que existan personas de por medio que posean nuestros datos. Esta tecnología permite realizar las transacciones sin intermediarios, es decir, de una manera descentralizada. Blockchain presenta un gran abanico de posibilidades para su implementación y una de estas es el voto electrónico. Es tan habitual usar las redes centralizadas que es inconcebible intercambiar información en Internet sin que estos datos pasen por los sistemas centrales de las grandes empresas que en teoría podrían vender, borrar e incluso modificar la información [2].

[1] https://www.cti.espol.edu.ec/node/20

1.1 Descripción del Problema

La ESPOL en la actualidad ha manejado un sistema de votación electrónica donde los votantes se acercan a un recinto electoral y mediante una máquina de votación eligen al candidato de su preferencia. Pero este mecanismo implica que los datos son manejados de forma integral por una sola entidad o grupo de personas asignadas para este propósito. Todo este proceso no ha estado exento de quejas de supuestos fraudes por grupos políticos involucrados debido a que no existe un seguimiento en tiempo real de los votos, esto quiere decir que los resultados parciales o totales no pueden ser vistos por los actores participantes sino hasta el final del conteo manual[2].

El voto electoral se lleva a cabo de manera electrónica, pero el conteo se realiza de forma manual usando muchas papeletas de votación, sin embargo, es posible que haya personas interesadas en manipular los resultados de las votaciones a su conveniencia. Esto quiere decir que el programa que se diseñará debe contar con muchas seguridades para que no se lleven a cabo estos delitos.

Los principales requerimientos del programa de votación electrónica se dan en la parte de seguridad y verificabilidad de los votos [3]. En ese sentido los adelantos en las tecnologías de la información juegan un papel clave en la evolución de estos procesos electorales. Desde hace algunos años muchas universidades en el mundo han implementado mecanismos y sistemas que permiten el voto electrónico, con el fin de mejorar la confianza en una votación [2].

1.2 Justificación

Mediante el mapa de experiencia del usuario (votantes) se pudo identificar insatisfacciones o experiencias negativas que tienen con el sistema de votación electrónica actual. La ESPOL posee una rigurosa penalización a los estudiantes empadronados que no votan, pero existen quejas por parte de los votantes que indican que muchas veces por falta de tiempo u olvido no pueden acudir al recinto electoral, lo que incrementa los niveles de ausentismo. La accesibilidad por parte de los estudiantes discapacitados y los que trabajan es otra insatisfacción identificada en el mapa de

[2]https://www.eluniverso.com/2012/08/25/1/1445/estudiantes-espol-pidieron-respeto-voto.html

experiencia; los primeros indican que es por su discapacidad y los segundos que por su horario de trabajo se les imposibilita ejercer su derecho al voto. Asimismo, el personal administrativo y docente manifiesta como experiencia negativa los elevados niveles de stress el día de la votación ya que tienen que estar pendientes de la fecha y hora. Por último las agrupaciones políticas presentan experiencias negativas debido a la inexistencia de un mecanismo de seguimiento electoral en tiempo real.

Basados en este contexto inferimos que la implementación de una red descentralizada Blockchain permitiría cambiar la idea tradicional del usuario respecto al funcionamiento y divulgación de resultados de elecciones. Se mejora y garantiza la seguridad en el desarrollo del proceso y genera un alto grado de confianza entre los actores involucrados [4].

1.3 Objetivos

1.3.1 Objetivo general

Diseñar una aplicación descentralizada de voto electrónico mediante el uso de la tecnología Blockchain para la confiabilidad del votante y de entidades electorales enfocados a comicios académicos.

1.3.2 Objetivos específicos

- Comprender el funcionamiento de la tecnología Blockchain utilizando un esquema de una red Ethereum para la implementación de una aplicación descentralizada.
- Implementar contratos inteligentes utilizando herramientas open source que permitan la ejecución de un sistema transaccional de votación electrónica.
- Comparar un sistema de voto tradicional con uno electrónico mediante métricas de satisfacción del usuario para la justificación de cambios en procesos electorales.

1.4 Marco Teórico

El voto es una herramienta importante para la toma de decisiones en grupos, empresas u organizaciones sobre todo cuando estas involucran información sensible o decisiones

monetarias. En la actualidad es muy común ver como este tipo de organizaciones tienen principalmente dos métodos para realizar sus procesos de votación, mediante software que les facilite la planeación y desarrollo de las votaciones o por medios más convencionales como el papel, que a pesar de ayudar a la auditabilidad de las votaciones se presta para problemas de seguridad y de planificación. Además de esto, en la actualidad por situaciones como la pandemia y el confinamiento causado por el Covid-19 alrededor del mundo, las metodologías de votación en varias empresas u organizaciones han cambiado. Las votaciones en papel no son igual de efectivas y en muchos casos no se pueden realizar, por estas razones se considera al e-voting como una alternativa para estas situaciones [5].

La tecnología Blockchain o cadena de bloques se originó como una alternativa al dinero fiduciario y sus aplicaciones van más allá de una herramienta para monedas digitales, convirtiéndose en el nuevo ecosistema de intercambio de información. Actualmente, estamos viviendo en una sociedad global en busca de implementación de tecnologías y del beneficio común, donde el Internet ha jugado un papel importante para la supervivencia del mundo empresarial y estatal, pero muchas exigencias y demandas no solo requieren de un intercambio de información, sino de poder realizar transacciones de valor seguras, transparentes y confiables, por lo que surge el Blockchain, como una solución para el desarrollo de los sectores económicos y sociales [6].

Blockchain también denominado por algunos “el nuevo Internet” que ganó impulso con la era de la industria 4.0 viene ganando mucha fuerza, sin embargo pocas personas entienden realmente cuáles son las aplicaciones y casos reales donde esta tecnología se puede desplegar. Una de estas aplicaciones es el voto electrónico, actualmente este sistema se basa en un acercamiento físico del votante y el resultado es administrado por una entidad centralizada, normalmente el gobierno, de esta manera se crea la confianza en éste ente. Asimismo permite garantizar el anónimato de la persona que sufraga e integridad del voto. Por ello gracias a la disponibilidad pública y registros distribuidos en todos los nodos de la red. Dado que un sistema de votación se desarrolla bajo sistemas democráticos, se entiende que un buen voto bajo esta modalidad debe tener 3 características principales: Privacidad: el voto debe ser secreto. Único-Elegibilidad: el voto debe ser asociado a una persona quien puede votar una sola vez. Verificabilidad: capacidad de verificar y confiar en el conteo de votos sin conocimiento especializado [7].

El costo de una elección es muy elevado, se tiene que crear papeletas, organizar toda la infraestructura necesaria para gestionar los votos y el posterior conteo de los mismos. Aunque ya se han probados sistemas de voto electrónico, estos han sido incapaces de cubrir todas las vulnerabilidades de ataques de hackers y/o de asegurar un conteo preciso, cosas no menores cuando muchas veces de eso depende el futuro de un país. La Blockchain puede ser una solución ya que permitiría un sistema de voto en el que las identidades de los votantes estuviesen protegidas, sean infalsificables y a un coste prácticamente nulo y de acceso público. Convirtiendo los votos en transacciones se puede crear una cadena que lleve cuentas de los votos, de esta manera todos pueden estar de acuerdo en el conteo final porque las cuentas es validada por nosotros mismos (votantes) y también verificar que ningún voto ha sido cambiado o removido y ningún voto ilegitimo ha sido agregado. Los problemas de ciberseguridad podrían acabarse con el sistema criptográfico del Blockchain, que permitirá sortear la suplantación de identidad de los votantes y mejorará la comodidad y la democratización del sistema electoral [8].

Hoy existen ya sistemas de voto electrónico llevados a producción, el caso más conocido es el de Estonia que desde el 2005 su plataforma de voto por Internet llamado: i-voting esta disponible [3], fue usado por el 44 % de los votantes en las últimas elecciones del 2019. Estonia es un claro ejemplo a seguir por sus resultados exitosos, a pesar de no haber utilizado una tecnología más segura como Blockchain. En Turquia también se utilizó el sistema de votación haciendo uso de tecnología Blockchain con resultados positivos. Este sistema trabaja bajo un flujo de procesos bastante sencillo: Autenticación - Registro - Verificación de distrito - Selección de candidato - Confirmación - Transacción. También indican las vulnerabilidades del diseño, reflejando que es un 51 % propenso a ataques cibernéticos, aunque para que estos se lleven a cabo se necesita hardware a gran escala, pero los resultados de las investigaciones concluyen que la probabilidad de ser atacados es bastante baja. Los expertos aseguran que un sistema basado en Blockchain presenta una solución para eliminar todas las desventajas del sistema de voto convencional, garantizando seguridad, integridad y velocidad en los resultados [9].

CAPÍTULO 2

2. METODOLOGÍA

El voto electrónico se ha vuelto un servicio esencial para los ciudadanos durante la pandemia y surge como consecuencia lógica de las medidas de distanciamiento. La reacción lógica y natural ante estas acciones durante la pandemia ha sido el uso de la tecnología como herramienta alternativa para continuar realizando, de forma remota, muchas de las actividades que tradicionalmente se han llevado a cabo de manera presencial[1]. Las autoridades electorales se han visto en la obligación de adaptar los procesos electorales a la "nueva normalidad". Las entidades electorales se han visto en la obligación de pensar en modalidades alternativas a la manera tradicional en la que se organizan y desarrollan elecciones. El éxito o fracaso del uso de herramientas tecnológicas en los comicios, particularmente el voto electrónico, depende, en gran medida, de la idiosincrasia de la población, de sus condiciones políticas, de su desarrollo, de la tradición y de la práctica electoral. Estas decisiones no pueden ser tomadas de manera unilateral o a puerta cerrada, debe haber un proceso abierto de consultas que incluya a todos los actores relevantes.

En esta sección se describe la arquitectura necesaria para diseñar el sistema de votación propuesto. Las consideraciones que se tuvieron en cuenta para que el sistema sea escalable a elección gubernamental. El flujo de la comunicación teniendo en cuenta donde se originan y terminan almacenadas. Para finalizar se hace una descripción de las funcionalidades ofrecidas por el sistema de votación y la tecnología utilizada para su implementación.

[1] https://www.excelsior.com.mx/opinion/francisco-guerrero-aguirre/el-voto-electronico-y-la-pandemia/1389727

2.1 Métricas a considerar

El tipo de métrica con la que se pretende evaluar la aplicación dada la arquitectura de micro-servicio utilizada es una métrica de procesos. Teniendo en cuenta que el micro-servicio diseñado consta de 5 procesos se estableció como métrica primaria el tiempo de respuesta de cada proceso(latencia). Además se estableció como métrica secundaria el gas utilizado por cada proceso del micro-servicio [10].

2.2 Blockchain: Nueva seguridad

Tradicionalmente, la base de datos con información de los resultados ha sido mantenida por una autoridad central u organización que tiene el completo control de la misma. Este ente que es la entidad electoral responsable de la elección tiene la capacidad de manipular los datos. Usualmente la autoridad mantiene la base de datos en el mismo lugar que fue creada. Si bien esta organización no tiene motivos para falsificar sus propios datos. Pero cuando involucra cuestiones financieras o datos sensitivos como el voto, no se desea dar un completo control de la base de datos a una autoridad u organización.

Aun si la organización garantiza no hacer ningún cambio fraudulento a la base de datos, es fácil para un hacker atacar una base de datos central. Para evitar tal situación, Blockchain hace la base de datos pública, donde todos los participantes en la elección pueden almacenar una copia individual de la base de datos que puede siempre ser comparada para chequear manipulaciones. Cuando una copia individual de la base de datos necesita ser actualizada Blockchain utiliza mecanismo de consenso [11].

2.3 Soluciones frente a un ataque cibernético

La gran debilidad de un sistema informático es que sea hackeable [12]. Blockchain evita que esto suceda y no lo hace con un firewall, ni con un buen antivirus, se auto protege gracias a su propia estructura, su arquitectura. Blockchain significa cadena de bloques y precisamente esto es, una cadena de bloques que contiene información. Cada bloque puede contener diferentes tipos de información en el caso de Bitcoin por e.g., la primera información que contiene es relativa a las transferencias de dinero como el

emisor, receptor, cantidad etc.; la segunda es el Hash, este es el número de identificación del bloque, se trata de un número único e irrepetible cada uno de los bloques tiene el suyo, y también tiene el Hash del bloque anterior por lo que cada uno de estos queda conectado con su predecesor y su sucesor. Los bloques van creando una cadena, podemos decir que Blockchain es inhackeable por dos características, la primera el Hash y la segunda que muchos ojos están mirando todo el rato. El Hash es el número único de cada bloque pero tiene una peculiaridad el número se genera según el contenido del bloque, eso significa que si se cambia el contenido del bloque, la información automáticamente cambia el Hash, imaginémoslo como una pieza de puzzle, con tal información tendrá tal forma, si alguien cambia la información la forma también cambiará, por lo que dejará de encajar y la cadena quedará invalidada. No es que haya una única base de datos, cada usuario tiene una copia de ella, dado que muchos ojos están mirando todo el rato. Si un usuario altera la información de su copia la comunidad lo sabe por lo que su versión de la base de datos es anulada y queda sin efecto. Ahí es donde radica la diferencia, la seguridad y la certificación de los documentos en Blockchain se la dan los usuarios [13].

Adicionalmente día a día surgen nuevas brechas y oportunidades en estas tecnologías para que los atacantes exploten. El aumento de las organizaciones cibernéticas dedicadas a estas labores trae consigo ataques cibernéticos más específicos y complejos de combatir ya que se está usando malware más sofisticado. Estos ciberdelincuentes están tratando de robar datos valiosos, como propiedad intelectual (PI), información personal identificable (IPI), registros de salud, datos financieros y además se está recurriendo a estrategias altamente rentables como monetizar el acceso a los datos a través del uso de técnicas avanzadas de ransomware o interrumpir las operaciones generales de la empresa a través de ataques distribuidos de negación del servicio [14].

2.4 Modelamiento de la Aplicación

2.4.1 Arquitectura

La Figura 2.1 muestra un esquema simplificado de la arquitectura necesaria para implementar el sistema de votación propuesto. La aplicación corre sobre un emulador Android que funciona con Flutter. El front-end permite interactuar con el sistema de

voto y monitorear los eventos de la Blockchain. El back-end trabaja como micro-servicio mediante comunicación REST y permite manejar todos los detalles para crear elecciones y votos. El servicio de autenticación es proveído por la ESPOL permitiendo la validación de los votantes.

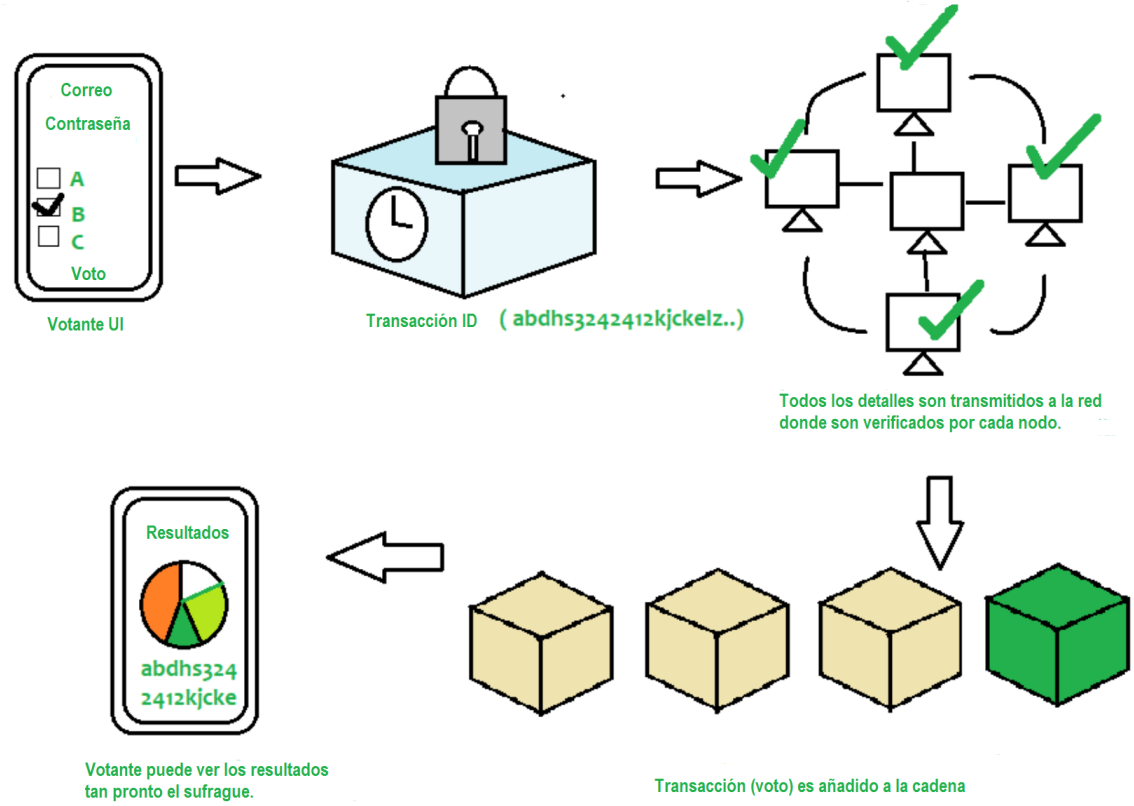

Figura 2.1: Arquitectura del sistema de votación propuesto

2.4.2 Consideraciones

Es importante antes de elaborar un diseño tener en cuenta todas las consideraciones para construir un buen sistema de voto electrónico. Después de evaluar el sistema de voto electrónico actual, y analizar los requerimientos para que un sistema sea efectivamente escalado a elección gubernamental, se construyó la siguiente lista de consideraciones a tener en cuenta para que un sistema de voto sea viable [11]:

- El sistema de voto electrónico debería identificar la identidad del votante y autentificar solo votantes elegibles.

- El sistema de voto electrónico no debería permitir acceso a candidatos inválidos.
- Cualquier votante debería tener solo una oportunidad para votar por ejemplo el sistema tiene que prevenir el doble voto.
- Debería proveer completa privacidad al votante y los votos no deberían ser rastreables.
- El sistema no debería permitir la manipulación de los votos por nadie.
- El sistema no tiene que permitir a una simple autoridad controlar el conteo.

2.4.3 Actores

Durante un proceso electoral participan los actores diferenciados por las tareas y permisos que tengan para llevar a cabo una votación exitosamente. A continuación se detallan los actores que participan en el proceso de votación electrónica:

2.4.3.1 Votante

Persona que participa en el proceso de votación emitiendo el voto como opción. Para el caso de la prueba que se presenta sería un ciudadano con derecho a voto que emite la elección del candidato elegido. El votante interactúa directamente con la aplicación del cliente, la cual es una aplicación móvil a la que acceden los ciudadanos para participar en el proceso.

2.4.3.2 Entidad Electoral

Es el ente responsable de la organización del proceso de votación, encargándose de definir las reglas que lo rigen con el objetivo de garantizar la transparencia y objetividad durante todo su desarrollo. Además es la organización que se encarga de autenticar la identidad de los votantes para decidir si pueden votar o no. La figura 2.2 muestra el proceso de votación detallado con los diferentes actores electorales.

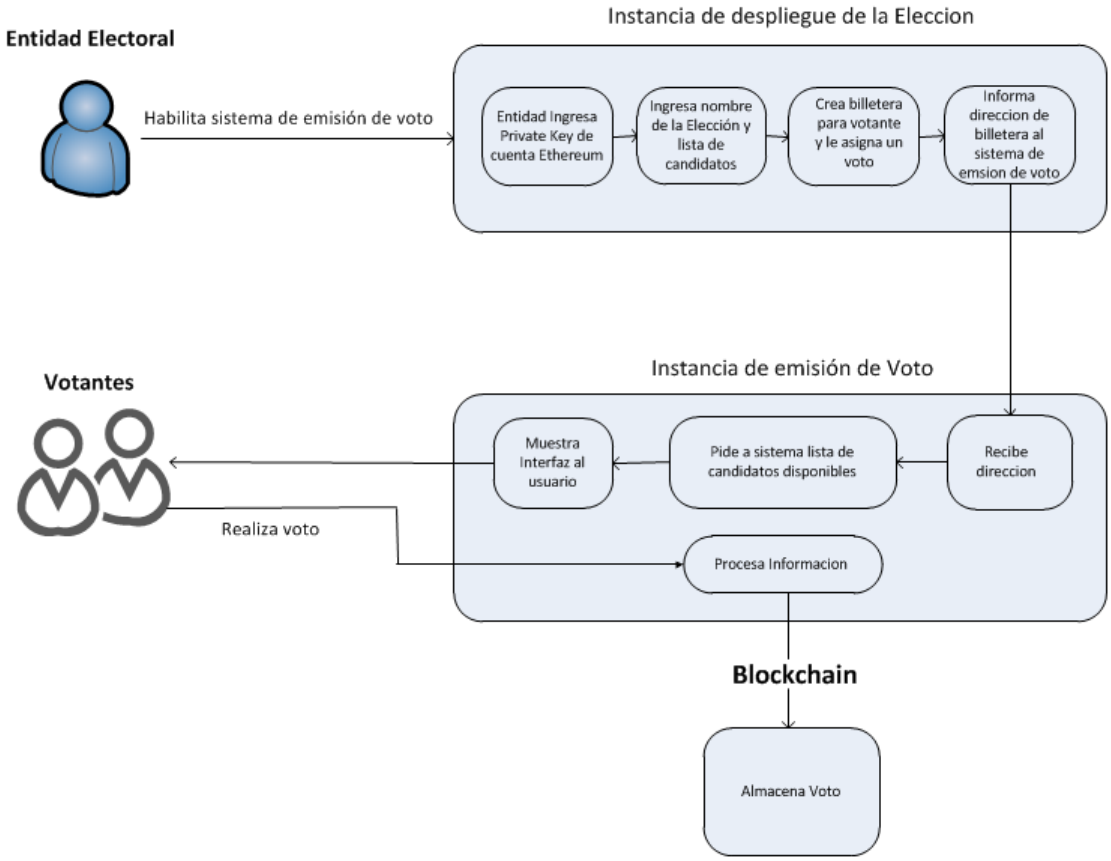

Figura 2.2: Interrelación de Actores

2.4.4 Políticas Generales

Las políticas, regulan la descarga, el acceso y el uso de la aplicación móvil para votación electrónica. Además establecen los derechos y restricciones que le son aplicables a quien descargue o use la aplicación en dispositivos móviles aptos para ello, como teléfonos inteligentes o tabletas:

- El acceso y descarga de la aplicación es gratuito salvo en lo relativo al coste de la conexión a través de la red de telecomunicaciones suministrada por el proveedor de acceso contratado por los usuarios.
- La aplicación obtiene la información que usted proporciona cuando se descarga. Para utilizar sus servicios deberá proporcionar previamente ciertos datos de carácter personal como son el correo y la clave que solo serán utilizados para el propósito de la votación.

- El Votante se compromete a utilizar la presente aplicación móvil y su servicio de conformidad con la ley, la moral, el orden público y las condiciones particulares que, en su caso, le sean de aplicación.
- El Votante se hace responsable de no difundir, transmitir o poner a disposición de terceros cualquier tipo de información, que suponga un sesgo electoral en los comicios.
- La Entidad electoral se compromete a garantizar y proteger las libertades públicas y los derechos fundamentales de los candidatos y los votantes guardando en absoluto secreto la información entregada por los usuarios.
- La prestación de los servicios de la aplicación móvil estará disponible solo mientras dure las elecciones.

2.5 Flujo de Comunicación

El proceso de registro de los votantes y candidatos es realizado con anterioridad por la entidad dueña de la elección, todo esto antes de proveér la aplicación móvil a los votantes. La verificación de identidad también se recomienda que debe ser hecha antes de crear las cuentas Ethereum. Después de validar la identidad de los usuarios, la entidad electoral debe autenticar a los votantes elegibles proporcionando una cuenta Ethereum. Usando esta cuenta, cada usuario puede votar solo una vez. El proceso de verificación del contrato inteligente desplegado en Blockchain asegura que el doble voto no es posible, entonces ningún usuario puede votar dos veces. El sistema de voto electrónico con Blockchain es descentralizado. No hay autoridad central que regula, cuenta o administra las elecciones, esto significa que, ni siquiera el dueño de la elección puede alterar los resultados. Es importante mencionar también, que las responsabilidades de la entidad se limitan a:

- Desplegar la elección
- Agregar los candidatos
- Autorizar a los votantes

- Autenticar a los usuarios autorizados
- Proveér las cuentas Ethereum
- Y Distribuir la aplicación móvil

Las responsabilidades o funciones del usuario (votante potencial) son:

- Abrir la aplicación antes proporcionada
- Iniciar sesión con sus credenciales
- Emitir su voto
- Dar siguiemento de los resultados (opcional)

La ventaja de este flujo es la gran adaptabilidad que puede llegar a tener, ya que, las funcionalidades serian las mismas para cualquier proceso electoral, desde académicos, empresarial o privado hasta la mayor escala posible, gubernamental.

2.5.1 Diseño de la red

El diseño que se implementa para facilitar el funcionamiento de la aplicación es el de un servidor central donde se va a ejecutar el micro-servicio, que se usa como intermediario entre nodos. Con el fin de conocer como se relacionan los diferentes componentes del sistema que se está desarrollando, se presenta un diagrama de componentes para ver las diferentes interrelaciones, tal como se aprecia en la figura 2.3. La misma figura muestra como trabaja el flujo de datos, teniendo en cuenta donde se originan, mediante las acciones de un usuario, y donde terminan almacenados que es en la Blockchain de Ethereum.

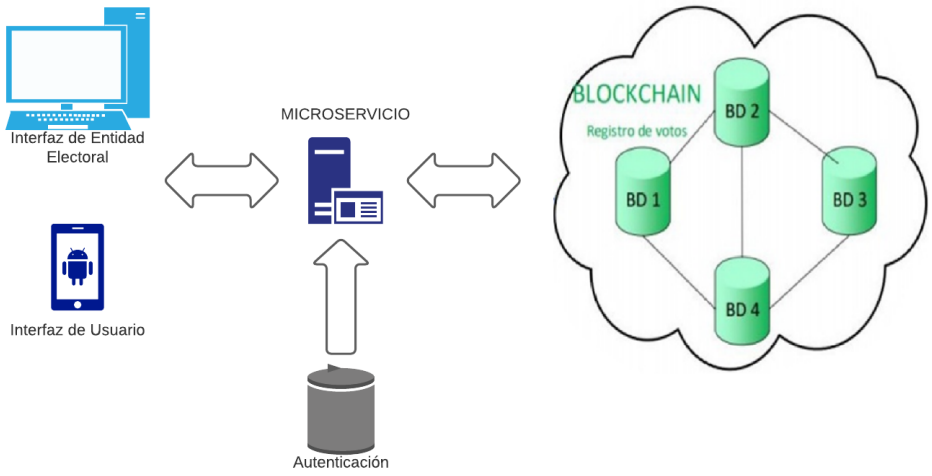

Figura 2.3: Diagrama de comunicación entre módulos del sistema

2.5.2 Contratos Inteligentes

Blockchain con los contratos inteligentes, emergió como un buen candidato para desarrollar el sistemas de votación electrónica más seguro, barato, transparente y fácil de usar. Ethereum y su red es una de las más adecuadas, debido a su consistencia, uso generalizado y provisión de lógica de contratos inteligentes. Se desarrollo una aplicación para el voto electrónico, basada en Blockchain usando la red Ethereum y los contratos inteligentes, y se considera que los votantes puedan usar aplicaciones móviles multiplataforma efectuar sus votos. El contrato inteligente está programado en Solidity el lenguaje mas popular [10]. Estos son una colección de estados y funciones, similares a una clase de Programación Orientada a Objetos. Cuando el contrato es desplegado, se les asigna una dirección para llamar las diferentes funciones públicas propias, que representan la lógica de negocio en una aplicación descentralizada (DApp). Los contratos inteligentes ayudan a realizar acuerdos y transacciónes de una manera confiable entre partes desconocidas sin la necesidad de una autoridad central.

2.5.3 Transacciones

Las transacciones son el elemento fundamental del sistema ya que esto permite la transmisión del voto entre el usuario y el candidato electoral. Las transacciones en la Blockchain están ligadas secuencialmente debido a que cada una de ellas incorpora

el hash de la transacción anterior y la clave pública del próximo. De esta manera, un conjunto de transacciones forman un bloque que está ligado secuencialmente haciendo referencia al hash del bloque anterior de la Blockchain. Así, si un atacante modifica cualquier dato de la cadena de bloques, daría como resultado un hash diferente en el bloque de dicha transacción modificada, con lo cual sería inmediatamente identificada la entidad atacante. Para poder alterar el contenido de una transacción o añadir información a la Blockchain, es necesario que la mayoría de los nodos lleguen a un consenso en común. Para ello, se emplean algoritmos de consenso como Proof-of-Work (PoW) y Proof-of-Stake (PoS). Mientras que PoW se basa en un reto que tienen que resolver los nodos para procesar la transacción, por su parte, PoS se basa en que los nodos que tengan más monedas sean los más interesados en defender la red y en conseguir un buen funcionamiento del sistema.

2.6 Aplicación para entidad Gubernamental

Se tiene que saber antes de crear el diseño de la App para la entidad electoral el tipo de usuario que va crear y administrar la elección. Es requerido ciertos conocimientos técnicos en especial en lo concerniente al funcionamiento de una red Ethereum.

2.6.1 Funcionalidades

La App de voto electrónico tiene las siguientes funcionalidades del lado de la entidad electoral:

- Crear elección: En esta ventana la entidad electoral escribe o carga los datos de su cuenta Ethereum válida, adicionalmente le da nombre a la elección.
- Ingresar candidatos: La entidad electoral ingresa los nombres y apellidos de los candidatos autorizados a participar en la elección.
- Autorizar votantes: En esta ventana la entidad electoral ingresa la cuenta Ethereum de todos los votantes que van a participar en la elección.
- Resultados: La última ventana muestra los datos de los candidatos junto con los votos nulos y blancos.

2.6.2 Tecnologías y Servicios

El despliegue de la elección lo realiza la entidad electoral en una aplicación web y la tecnología recomendable para implementar este diseño debe ser un kit de desarrollo versátil que permita crear aplicaciones tanto web como móvil. Flutter es la tecnología idónea para este caso ya que al ser un framework multiplataforma también facilita la creación de aplicaciones Android como IOS sobre una base única de código. Los servicios que ofrece la aplicación son: crear, administrar y finalizar una elección remotamente, sin la necesidad de imprimir papeletas de votación.

2.7 Aplicación para usuarios

Fue imprescindible a la hora inclinarnos por la aplicación móvil entender las necesidades del público al que esta dirigida, por lo general estudiantes que trabajan, discapacitados o que no quieren hacer cola en el recinto electoral. Para el diseño de la presente App se asumió que el votante cuenta con conocimientos básicos en la descarga y uso de aplicaciones móviles. Es decir el funcionamiento de esta App nos permite una navegación sencilla y está centrada en hacer lo menos complejo posible la experiencia del usuario.

2.7.1 Funcionalidades

La App de voto electrónico que se desarrolla tiene las siguientes funcionalidades de lado del votante:

- Autenticación: El usuario debe ingresar su correo y clave que le fue proporcionada por la entidad electoral. En el caso que ingrese mal estos campos se le mostrara un mensaje de error.
- Seleccionar candidato: Una vez que el votante pasa el proceso de autenticación se le muestran la lista de los candidatos disponibles incluidos nulos y blancos, cuando el usuario elige un candidato se le muestra un mensaje preguntando si esta seguro de su elección.
- Resultados: En esta ventana el votante solo por única vez podrá acceder a los resultados de las eleccióne.

2.7.2 Tecnologías y Servicios

El usuario realiza el proceso de votación mediante una aplicación móvil. La aplicación será proporcionada por la entidad electoral mediante su página web institucional o ubicada en el App Store para ser descargada por el votante. Al igual que la App para la entidad electoral la tecnología que se usó para el desarrollo fue Fluter al ser un framework multiplataforma que nos permite implementar aplicaciones tanto para Android como IOS. El servicio que ofrece la aplicación es el de ejercer el derecho al voto desde el teléfono inteligente de manera remota sin que se requiera la presencia física en el recinto electoral.

2.8 Blockchain como alternativa tecnológica

En lo que va del 2020 la implementación de la tecnología Blockchain se aceleró, dando solución a las necesidades que presenta la nueva escena mundial. La cadena de bloques permite implementar de manera rápida soluciones tecnológicas más ágiles, eficientes y autónomas, que además aporten una mayor confianza. Aunque la adopción de la tecnología Blockchain, tanto en procesos gubernamentales, como institucionales había ganado terreno en los últimos años, la masificación de la cadena de bloques venía dándose de manera lenta. Sin embargo, las medidas de aislamiento que se tomaron a nivel mundial a causa de la pandemia por Covid-19 aceleraron la transformación digital prevista años atrás con la aparición de esta nueva tecnología. La aplicación de medidas sanitarias que obligaron a organizaciones alrededor del mundo a operar de manera virtual trabajando desde casa, así como los trámites cotidianos que tuvieron que acoplarse para que se realizarán desde el confinamiento, pusieron en evidencia, no solo el riesgo al que se exponen empresas e instituciones por la eventual fuga de información, sino el desafío que se debe enfrentar para implementar de manera rápida soluciones tecnológicas más ágiles, eficientes y autónomas, que además aporten una mayor confianza[2].

No es difícil de imaginar al alto costo que conlleva crear papeletas, organizar toda la infraestructura necesaria para gestionar las votaciones y el posterior conteo. Ya se han probado sistemas de voto electrónico, pero han sido incapaces de resistir ataques de hackers y de tener fallos a la hora de hacer el recuento con total precisión. Blockchain

[2]https://technocio.com/blockchain-la-alternativa-tecnologica-para-enfrentar-la-nueva-realidad/

podría solucionar esto ya que permitiría un sistema de voto en el que las identidades de los votantes estuviesen protegidas, infalsificable, a un coste prácticamente nulo y de acceso público [15].

CAPÍTULO 3

3. RESULTADOS Y ANALISIS

En esta sección se muestran los resultados del proyecto en el marco de la funcionalidad ofrecida a la entidad electoral y el votante. Los diferentes casos de uso que se realizaron a la aplicación web y móvil. Luego se hace análisis de las métricas cuantificables encontradas. Se muestra los resultados de una encuesta sobre la aceptación del voto por la población. Para finalmente analizar el presupuesto del costo para una posible implementación.

3.1 Aplicaciones

El resultado que se muestra es un sistema que consta fundamentalmente de dos partes. En primera instancia, una aplicación web donde la entidad electoral despliega la elección. Y por otro lado se tiene una aplicación móvil donde el usuario emite su voto. El proceso de autenticación lo proveé la entidad electoral o dueño de la elección, sin embargo, para la prueba que se realizó se creó un servicio de autenticación que consulta a una base de datos mariaDB con 10 usuarios (correo y contraseña). El votante para usar el sistema debe se validado antes por la entidad electoral, es decir, ya debe estar registrado.

La interfaz de usuario de las aplicaciones que se proponen en las pruebas son sumamente simples, ya que, se pretende que el despliegue de las mismas sean bajo demanda, lo que permite escalabilidad y adaptabilidad. Tan solo se logro tener 10 usuarios, dado que, es el máximo número de cuentas ethereum que proporciona Ganache, una aplicación de escritorio que permite desarrollar, implementar y probar aplicaciones descentralizadas bajo un ambiente local, seguro y sin costo alguno.

3.1.1 Aplicación Web

La entidad electoral para desplegar una elección en su aplicación web necesita una PC, laptop, teléfono inteligente o tablet, que cuente con un navegador basado en chromium y con conexión a Internet (de preferencia cableada).

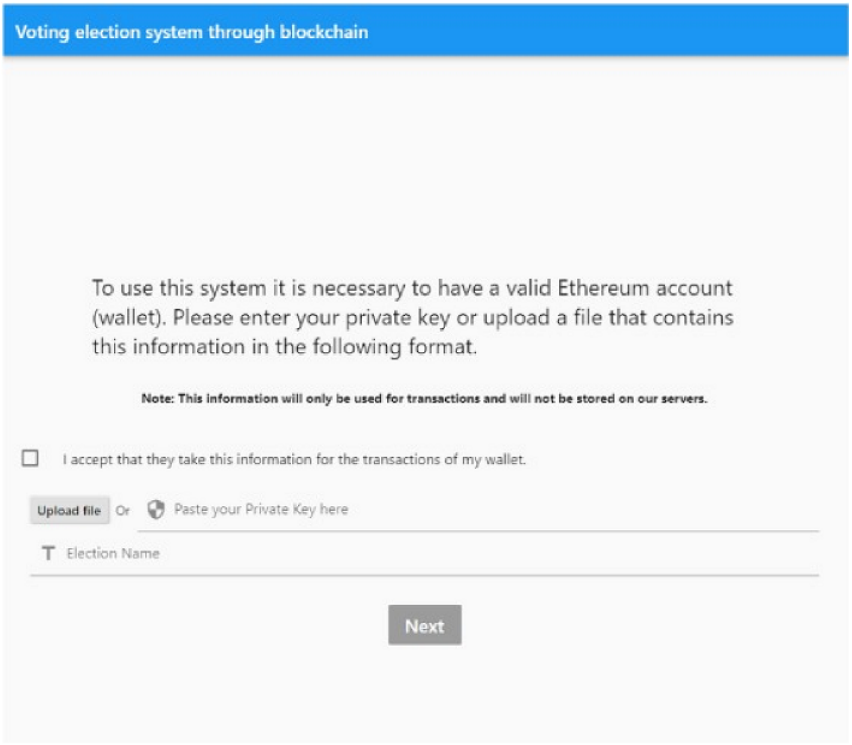

Figura 3.1: Aplicación Web para la entidad electoral

3.1.2 Aplicación Móvil

El usuario que va a emitir su voto requiere de un teléfono inteligente con conexión a Internet, ya sea via Wi-Fi o a traves de un plan de datos.

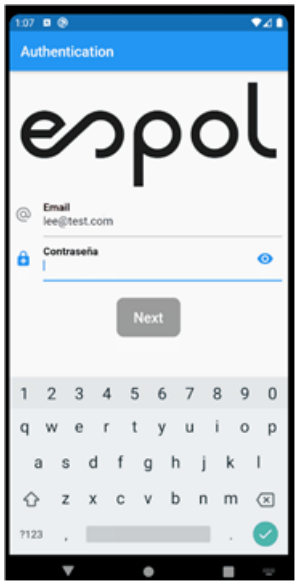

Figura 3.2: Aplicación móvil para el votante

3.2 Pruebas de rendimiento

El proceso de prueba se ha convertido en una tarea vital dentro del desarrollo de cualquier sistema informático. Es por esto último que, para estresar el sistema, se siguió el patrón de pruebas unitarias, es decir, se probaron las principales funcionalidades del micro-servicio de manera aislada tratando de mantener parámetros semejantes para el ambiente donde se llevaron a cabo. Apache JMeter fue la herramienta para simular los siguientes escenarios con diferentes cargas para todo el sistema:

1. Baja escala, limitaciones dadas por el ambiente de prueba.
    - Número de usuarios simultáneos: 10
    - Periodo de aceleración: 10 segundos
    - Recuento de bucles: 10
2. Mediana escala.
    - Número de usuarios simultáneos: 100
    - Periodo de aceleración: 10 segundos
    - Recuento de bucles: 10
3. Gran escala, caso ESPOL

- Número de usuarios simultáneos: 10000
- Periodo de aceleración: 10 segundos
- Recuento de bucles: 10

Es importante aclarar que el recuento de bucles es la cantidad de veces que cada usuario ejecutaría la prueba, el periodo de aceleración es lo que JMeter tarda en poner a los usuarios en funcionamiento, también de que en el host donde se realizó el estrés está montada toda la arquitectura.

DESPLIEGUE DEL CONTRATO INTELIGENTE						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
6.6/sec	360 ms	268 ms	No aplica	1077 ms	180 ms	1 seg

Tabla 3.1: Resultados de Apache JMeter: desplegar contrato

El proceso que despliega el contrato solo debe ejecutarse una vez y es sumamente controlado, ya que sin este proceso, los demás simplemente no se pueden ejecutar. Esto no significa que no se puede medir, también el formato y campos de la tabla 3.1 marcan las métricas que ofrece JMeter.

3.2.1 Escenario 1

Agregar Candidato						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
8.8/sec	260 ms	250 ms	0 %	612 ms	165 ms	15 seg
Autorizar Votante						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
9.9/sec	188 ms	183 ms	0 %	612 ms	102 ms	15 seg
Emitir Voto						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
9.9/sec	176 ms	137 ms	0 %	456 ms	126 ms	15 seg
Obtener Resultados						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
9.9/sec	269 ms	237 ms	0 %	621 ms	185 ms	15 seg
Autenticación del votante						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
1.1/sec	87 ms	77 ms	0 %	178 ms	74 ms	15 seg

Tabla 3.2: Resultados de Apache JMeter: Escenario 1

Este primer escenario es el único en el que se puede replicar en el ambiente de desarrollo, un ambiente controlado y muy sencillo de testear, es por esto que, no se tiene error alguno. También este es el único escenario donde se puede recrear todo el flujo de comunicación de manera exitosa.

Antes de avanzar, es importante mencionar que por facilidad de entendimiento y

explicación, el análisis de los resultados de JMeter en los tres escenarios se realiza al final de esta subsección.

3.2.2 Escenario 2

Agregar Candidato						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
9.7/sec	312 ms	305 ms	0 %	600 ms	141 ms	15 seg
Autorizar Votante						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
9.2/sec	293 ms	211 ms	0 %	1480 ms	106 ms	15 seg
Emitir Voto						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
9.9/sec	190 ms	183 ms	0 %	551 ms	81 ms	15 seg
Obtener Resultados						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
3.6/sec	13618 ms	16494 ms	0 %	18255 ms	1652 ms	15 seg
Autenticación del votante						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
10.0/sec	78 ms	74 ms	0 %	238 ms	71 ms	15 seg

Tabla 3.3: Resultados de Apache JMeter: Escenario 2

¿Qué sucede en este escenario? Lo mejor es que sigue sin haber errores, el rendimiento está cercano al ambiente de desarrollo pero, el tiempo de respuesta aumentó ligeramente

en todos menos en obtener resultados, en este último se dispara hacia arriba.

3.2.3 Escenario 3

Agregar Candidato						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
61.9/sec	91251 ms	107338 ms	99.98 %	151127 ms	0 ms	2:33 min
Autorizar Votante						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
64.0/sec	86246 ms	99582 ms	99.98 %	145989 ms	0 ms	2:33 min
Emitir Voto						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
65.2/sec	85141 ms	98427 ms	99.99 %	143789 ms	0 ms	2:33 min
Obtener Resultados						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
53.5/sec	14504 ms	180690 ms	100 %	187007 ms	0 ms	no aplica
Autenticación del votante						
Rendimiento	**Promedio**	**Mediana**	**Error**	**Máxima**	**Mínima**	**Duración**
319.6/sec	13366 ms	13523 ms	82.76 %	29522 ms	209 ms	32 seg

Tabla 3.4: Resultados de Apache JMeter: Escenario 3

En este último escenario, el micro-servicio se cayó dos veces, pero gracias a que está configurado con un sistema de recuperación, volvió a estar activo en cuestión de milisegundos, el tiempo de inactividad fue tan bajo que JMeter no lo detecto, por ende,

se asume como despreciable.

```
POST /get-stats HTTP/1.1
Host: localhost:8080
Connection: keep-alive
Content-Length: 73
Content-Type: text/plain
User-Agent: Apache-HttpClient/4.5.12 (Java/1.8.0_242-release)
```

Figura 3.3: Registros: micro-servicio down

3.2.4 Análisis de la métricas de JMeter

- Rendimiento, indica la cantidad de peticiones que el micro-servicio puede manejar.
- Promedio, representa la latencia promedio del servicio.
- Mediana, latencia de una muestra(usuario) que está en medio de las n muestras registradas.
- Error, porcentaje de respuestas con Código de estado de respuesta HTTP diferente a 200.
- Máxima y Mínima, valores de latencia que se explica solo con el nombre.
- Duración: Tiempo que le tomó JMeter ejecutar el test.

En los tres escenarios, JMeter muestra que el micro-servicio puede manejar diversas escalas de peticiones, claramente existe un cuello de botella que es provocado por Ganache, que es el simula la pequeña red blockchain local con tan solo 10 cuentas Ethereum, transacciones y peticiones limitadas. El porcentaje de error está presente cuando Ganache no responde exitosamente, ya que, no es capaz de manejar varias peticiones de manera paralela y lamentablemente esto nos impiden probar a gran escala.

Para la autenticación del votante se salva del cuello de botella, debido a que, Ganache no interviene, para el tercer escenario los errores presentados fueron a causa principalmente de la base de datos.

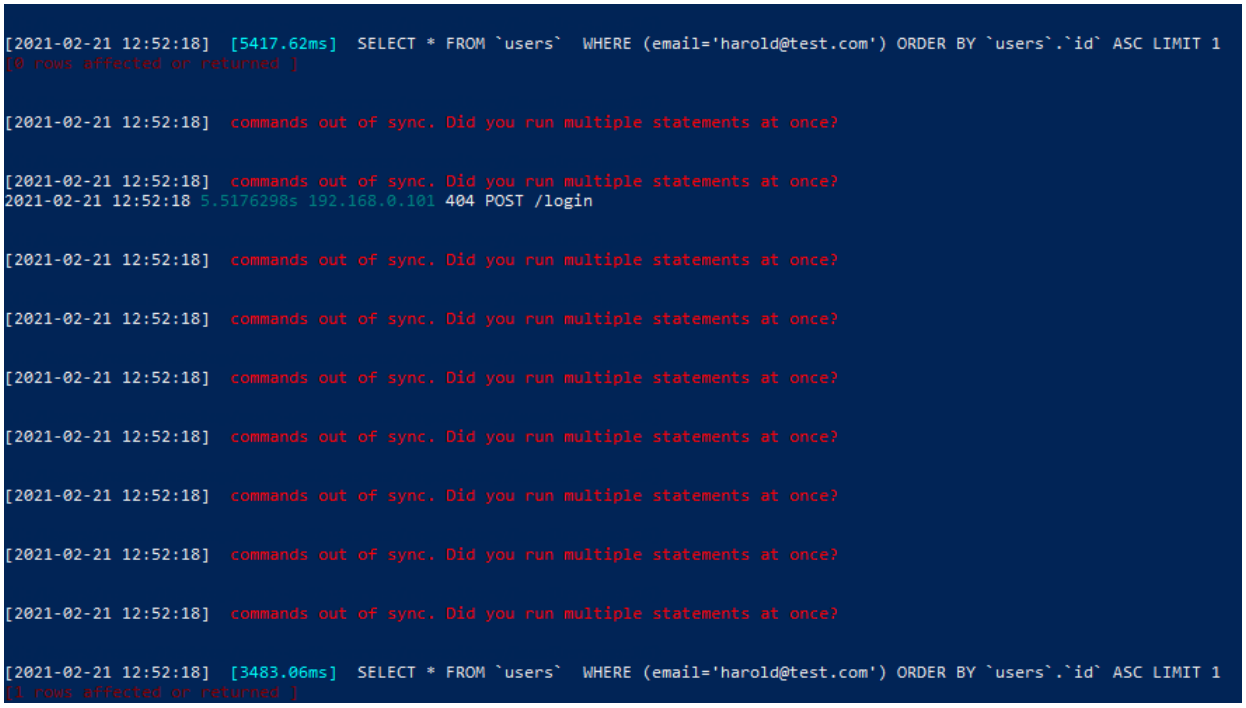

Figura 3.4: Registros: errores en DB

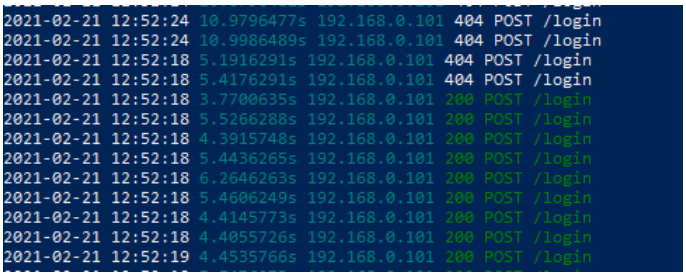

Figura 3.5: Registros: errores en DB

Tanto en la figura 3.4 como en la 3.5 se registra los errores y largos tiempos que le toma a la base de datos hacer una consulta sencilla cuando existe un alto número de peticiones, exactamente 10000. Esta base de datos y el servicio de autenticación es proporcionada por la entidad electoral y para el ambiente de pruebas se montó una API sencillo emulando dicho servicio y el proceso que se ejecutaba es autenticación del votante.

3.3 Métricas seleccionadas para producción

Una vez que el sistema informático pasa la fase de desarrollo y de prueba, es conveniente establecer métricas cuantificables que permitan medir el rendimiento del sistema. Dada la

arquitectura de micro-servicio y pruebas de rendimiento finalizadas, se procede a validar si los resultados de JMeter van acorde de un ambiente real, pero para determinar lo antes dicho, hay que entender a detalle cada proceso.

El micro-servicio que se desarrolló consta de cinco procesos, estos son de todo el sistema pero no todos pertenecen al votante, además en un ambiente de producción no se ejecuta el mismo número de veces, por ende, para un mejor análisis de las métricas seleccionadas se presenta el flujo de la arquitectura propuesta y sus respectivos identificadores.

Entidad Gubernamental: Entidad electoral o dueño de la elección, para el caso de prueba es la ESPOL.

Micro-servicio: Módulo que se encarga de hacer la conexión con la red Blockchain de Ethereum para ejecutar las transacciones.

Tx: La transacción o proceso en si.

Votante: El usuario final que emite el voto desde la apliación movil.

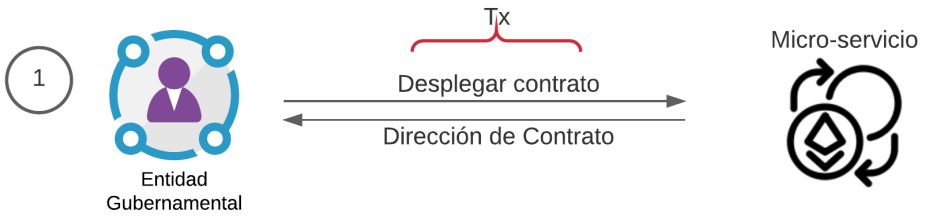

Figura 3.6: Desplegar elección

Ya se indicó que desplegar el contrato digital se hace una única vez, como muestra la figura 3.6, el despliegue de la elección es donde el contrato inteligente es enviado a la red de blockchain bajo las políticas que la entidad haya establecido, este primer proceso genera mayor costo en las métricas seleccionadas más adelante.

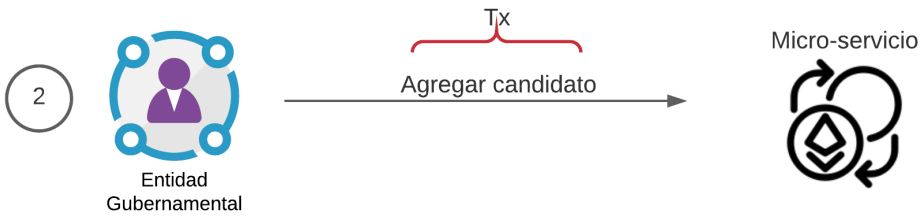

Figura 3.7: Agregar candidatos

Lo siguiente es agregar a los candidatos, mismo que se llevará a cabo o se ejecutará tantas veces como candidatos o partidos políticos exista. En un proceso electoral real, es muy raro ver que el número de opciones superen los 20, e.g., las últimas elecciones presidenciales en Ecuador del año 2021 se llevaron a cabo con 16 candidatos.

Esto significa que para este proceso, solo aplica el escenario 1 de las pruebas de rendimiento.

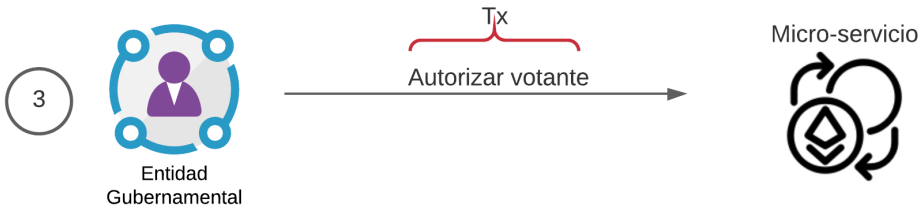

Figura 3.8: Autorizar votante

Luego de agregar a los candidatos, se procede a autorizar al votante, de la misma manera que el paso anterior se llevará a cabo o se ejecutará tantas veces como votantes exista. Para este proceso, aplica los tres escenarios de las pruebas de rendimiento, sin embargo, también como el anterior este es un proceso que debe ejecutar la entidad electoral, de manera controlada y de preferencia secuencial, es decir, registrar un votante a la vez.

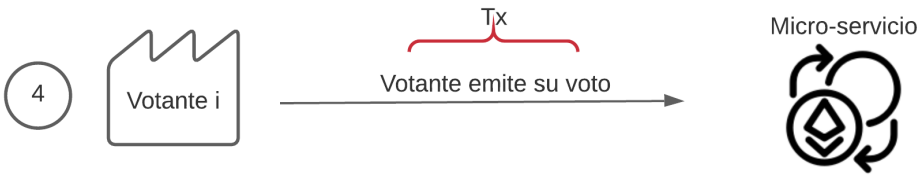

Figura 3.9: Votante emite su voto

Ya con los candidatos agregados y votantes autorizados, la entidad tiene que facilitar el aplicativo móvil a sus usuarios para que estos procedan a ejercer su derecho al voto. Acá no hay limitantes, ya que, depende de un comportamiento humano. También aplica los tres escenarios.

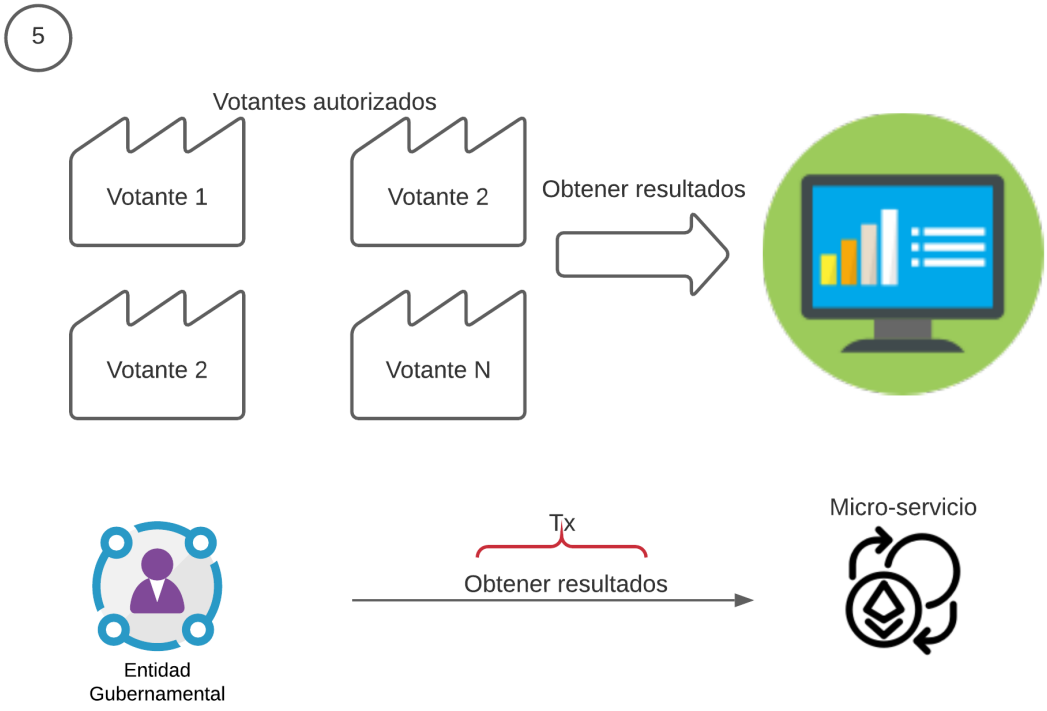

Figura 3.10: Obterner resultados

Obtener los resultados es el último proceso que también aplica a los tres escenarios, el costo en cuanto tiempo de respuesta es similar a los anteriores, sin embargo, el

gas es igual a 0, más adelante se muestran las gráficas comparativas para una mejor visualización.

3.3.1 Latencia de las funcionalidades del sistema

Una métrica importante para cualquier sistema donde conlleve una conexión entre dos o más puntos, es el tiempo de respuesta también conocido como latencia cuya unidad de medida es milisegundos(ms). Se realizó un análisis comparativo del tiempo de respuesta de cada proceso como muestra la figura 3.11 para estimar el rendimiento de la aplicación en un ambiente de producción

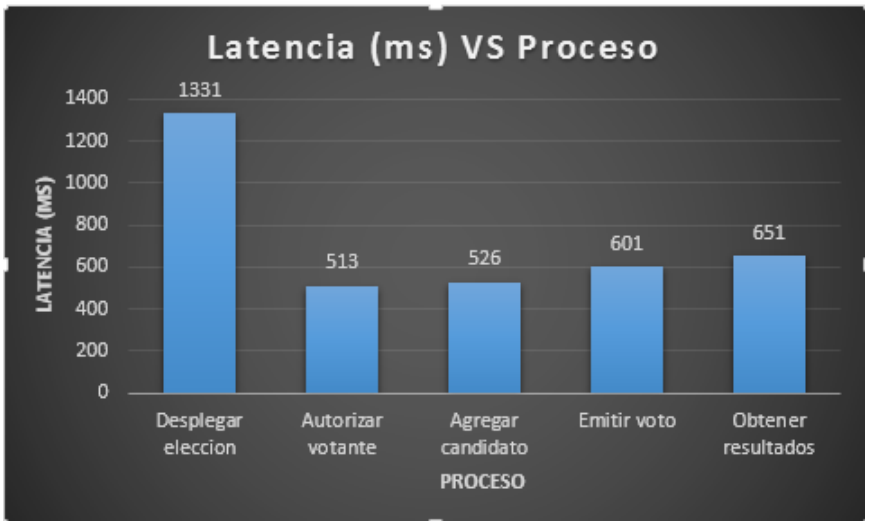

Figura 3.11: Latencia vs Proceso

Las pruebas de estrés fueron las máximas permitidas por el ambiente de pruebas y tambien para que den una respuesta exitosa, es decir, el proceso para desplegar elección se ejecutó una sola vez por escenario, mientras que los procesos: agregar candidato, autorizar votante y emitir voto se ejecutaron un número total de 10 veces. Por otro lado, obtener resultados se lo obtuvo promediando los tres escenarios, este último proceso solo requiere de la dirección del contrato inteligente y no necesita de una cuenta ethereum, por ende, se puede ejecutar un mayor número de veces sin generar mayores costos.

3.3.2 Tarifa por transacción en Ethereum: Gas

Las actualizaciones en la Blockchain se realizan a través de transacciones. Estas transacciones generan un costo medido en gas el cual es una medida del gasto

computacional de todos los nodos que escriben en la red, el gas es indistinto por usuario, es decir, la variación del gas usado depende del proceso o transacción y los nodos presentes en la red Block. La figura 3.12 muestra una comparativa del gas utilizado por cada proceso del micro-servicio.

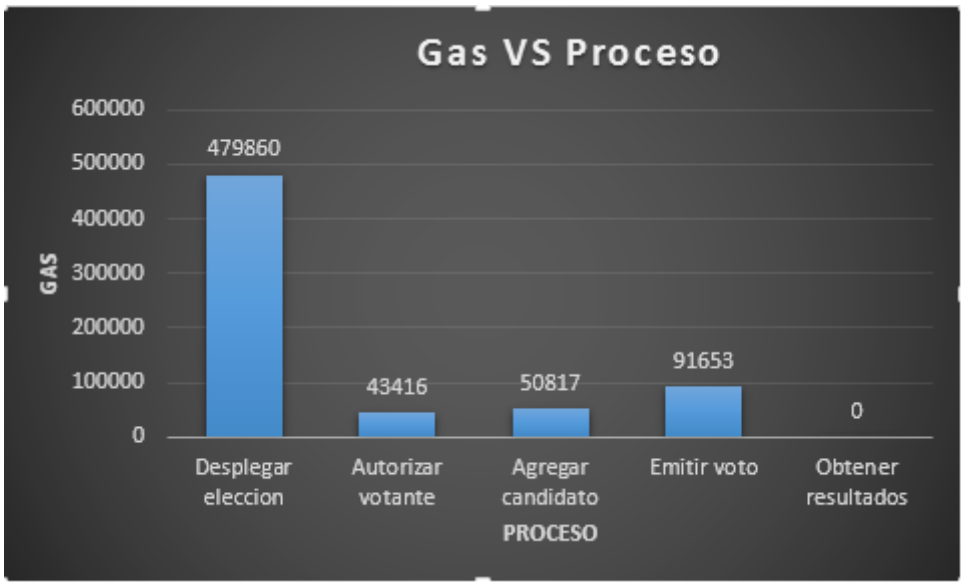

Figura 3.12: Gas vs Proceso

El gas es sumamente importante para cada transacción, ya que de este depende que tan rápido se realiza un proceso, también ayuda a estimar valores monetarios para el dueño de la elección en un ambiente de producción, es por esto que, se debe marcar un límite de gas por transacción y para el caso de prueba se marcó 3000000, ya que, es el máximo para ejecutar una transacción del contrato inteligente desplegado. El micro-servicio tiene gas variable para cada proceso con el fin de hacer el menor gasto posible, y como la Figura 3.12 presenta el gas mínimo es 0.

3.4 Encuesta

Los datos obtenidos de la encuesta realizada a 22 estudiantes de la ESPOL corresponden a un muestreo no probabilístico, solo para fines exploratorios. Se realizó 3 preguntas que buscan medir cuan satisfechos están los estudiantes con el sistema de votación electrónica actual, el nivel de confianza que se tendría si se implementa el sistema de votación remoto y el grado de conocimiento con respecto a la seguridad que aporta la tecnología Blockchain al voto electrónico. Cabe señalar que esta encuesta tenía como

objetivo el público en general, pero por carecer de los medios para llegar a esta población teórica(personal docente y administrativo), se centró en la población accesible, que son los estudiantes.

3.4.1 Confianza de los estudiantes en el sistema de votación actual

El objetivo de esta pregunta es medir el nivel de confianza que tienen los estudiantes en el sistema de votación electrónica actual. Considera usted que el sistema de votación electrónico actual es confiable:

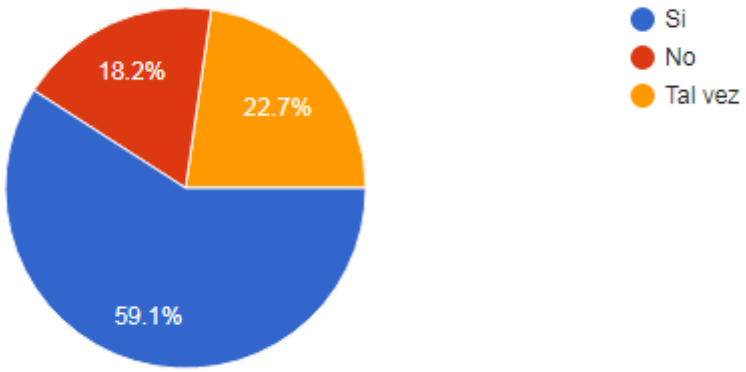

Figura 3.13: Confianza en el sistema de votación actual

Como se observa en la figura 3.13 de la encuesta realizada, el 59.1 % tiene confianza en el sistema de votación electrónico actual, el 18.2 % no confia en este sistema y el 22.7 % se encuentra indeciso.

3.4.2 Modalidad de votación electrónica

La meta de esta pregunta es conocer cuan seguros se sentirían los estudiantes al utilizar un sistema de votación remoto con respecto al sistema de votación actual. Que sistema de votación le parece mas confiable: 1- Remoto 2- Presencial 3- Ninguno.

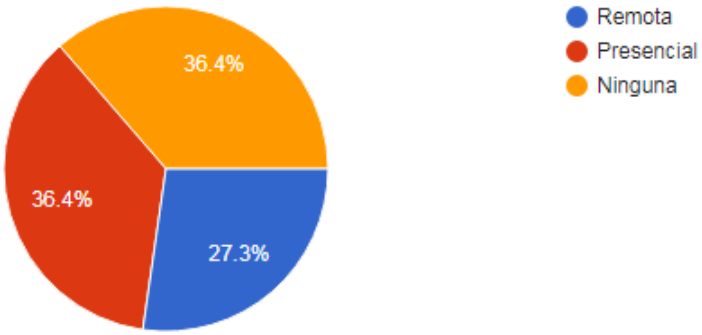

Figura 3.14: Modalidad de votación electrónica

Como se observa en la figura 3.14, el 27.3 % tiene confianza en el sistema de votación remoto, el 36.4 % sigue confiando en el sistema presencial mientras que el otro 36.4 % manifiesta no confiar en ninguno.

3.4.3 Confianza en el sistema de voto electrónico con Blockchain

El objetivo de esta pregunta es medir el conocimiento que tienen los estudiantes con respecto a la tecnología Blockchain aplicada al voto electrónico. Si compara el sistema de votación electrónica actual con el sistema de votación remoto usando tecnología Blockchain, cree usted que el voto es: 1- Mas confiable 2- Menos confiable 3- Igualmente confiable

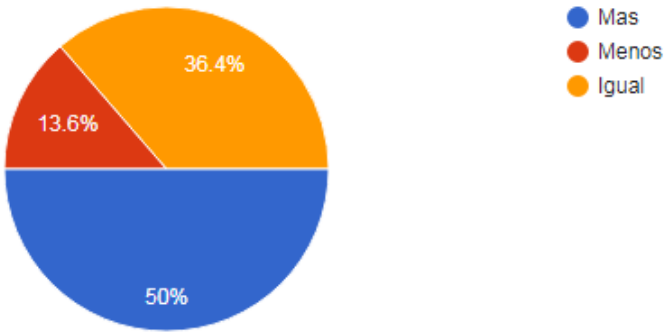

Figura 3.15: Confianza en el voto electrónico con Blockchain

Como se observa en la figura 3.15, el 50 % de los encuestados cree que el sistema

de votación electrónica con Blockchain sería mas confiable, el 36.4 % manifiesta que sería igualmente confiable, mientras que 13.6 % piensa que seria menos confiable. Estos resultados evidencian un alto grado de desconocimiento de los usuarios sobre la tecnología Blockchain, especificamente sobre sus aplicaciones al voto electrónico.

3.5 Analisis de Costos

A continuación se presenta los resultados de la factibilidad económica en la implementación de un prototipo a pequeña escala de una red descentralizada Blockchain para voto electrónico.

Cabe recalcar, el prototipo que se presenta en el documento es una base sólida con enfoque escalable, las estimaciones son bajo un ambiente de desarrollo y las limitaciones de las pruebas. Además el modelo de negocio pretendido es similar a PaaS o Plataforma como un servicio, lo que permite escalabilidad bajo demanda. Lo que significa que además de los aplicativos, se le brinda asesoramiento y soporte a la entidad interesada.

Tipo	Descripción	Costo
PC(s)	Equipos para desarrollar las aplicaciones	750 $
Programador(es)	Remuneración de talento humano	20 $ / hora

Tabla 3.5: Presupuesto: Ambiente de desarrollo o prototipo

Las características de hardware del equipo que se utilizó para realizar las pruebas son: Procesador Intel core i7 4tha generación, memoria RAM de 16 GB y disco duro de 500 GB en SSD. Estos parametros se pueden depreciar en la visión de la entidad a contratar/pagar por el software.

En la siguiente tabla se muestra una propuesta de despliegue a producción en los servicios de AWS (Amazon web service).

Tipo	Descripción	Costo-mes
Lambda function	Micro-servicio, el cobro es por ejecución	18.74 $

Tabla 3.6: Presupuesto: Ambiente de producción con 3 millones de ejecuciones al mes

No se ofrece requerimientos de un servidor, ya que, Lambda function es autoescalable y se ejecuta solo las veces que se lo llama, en cuanto a las limitaciones de este servicio es el tiempo máximo de ejecución: 15 minutos y memoria máxima de 10240MB.

Si este sistema de votación se lo desea escalar a una elección de mayor dimensión los costos aumentarian, ya que se tendría que comprar cuentas Ethereum con fondos para las transacciones. Con la propuesta mostrada en la table 3.2, misma que se obtuvo directamente de la calculadora provista por la página oficial de AWS, es mas que suficiente para los comicios académicos en ESPOl, dado que tienen alrededor de 10000 usuarios o estudiantes, claro esta, que en un ambiente real los tiempos de respuesta serian considerablemente mas bajos.

El costo verdaderamente significativo son las cuentas Ethereum, teniendo en cuenta que con fecha que se redacta este documento 1 Ethereum es igual a 1.846,41 dólar estadounidense se presenta el siguiente presupuesto bajo las estadisticas que resultaron del ambiente de prueba.

Proceso	**Costo en Ethers**	**Costo en USD**
Desplegar contrato	0.01072934 ETH	19.81 $
Agregar candidato	0.00093492 ETH	1.73 $
Authorizar votante	0.00087571 ETH	1.62 $
Emitir voto	0.00251401 ETH	4.64 $
Obtener resultado voto	0.000000001 ETH	0.0000018 $

Tabla 3.7: Presupuesto de cuentas Ether: Ambiente de desarrollo

Haciendo una extrapolación simple, a 10000 solicitudes para ESPOL con los costos del ambiente de prueba, el costo total sería de: 278,000.018 $

Otra opción viable sería montar una red local de Blockchain para evitar el costo en Ether por las cuentas y transacciones, aunque, se perdería confiabilidad.

CAPÍTULO 4

4. CONCLUSIONES Y LINEAS FUTURAS

En esta sección se describió la importancia del trabajo desarrollado, las fortalezas y debilidades. Se discute que medios o tecnologías harían falta si se desea escalar el sistema de votación propuesto a una elección gubernamental. Por último, se analiza las implicaciones de este proyecto en posibles trabajos futuros.

4.1 Conclusiones

- A través de un estudio del modelo de votación tradicional, se desarrolló un sistema de votación electrónica, en el que la entidad gubernamental puede desplegar una elección cumpliendo con los requisitos esenciales de un proceso electoral.
- Se diseñó un sistema de votación electrónica a pequeña escala, integrando los aspectos de infraestructura de moneda criptográfica Ethereum y la tecnología Blockchain. Este sistema permite crear una votación descentralizada y anónima asegurando la integridad de cada uno de los votos.

4.2 Recomendaciones

- Considerando la limitante que se tuvo con el cliente Ethereum, dado que este solo nos ofrecía 10 cuentas activas; se sugiere a la entidad electoral para implementar una votación a mediana o gran escala comprar cuentas Ethereum con fondos para las transacciones.
- Teniendo en cuenta que el sistema de votación propuesto no ofrece persistencia de los resultados una vez finalizada la elección, se recomienda a la entidad electoral

contratar un servicio de almacenamiento en la nube para respaldar los resultados de las elecciones.

4.3 Líneas Futuras

- El desarrollo de este proyecto ayuda a abrir la puerta para que la tecnología Blockchain logre establecerse en los próximos años en los sistemas de votación electrónica, y el votante sienta la confianza al momento de sufragar.
- En un futuro se plantea la posibilidad de desplegar el sistema de votación propuesto a gran escala, realizando pruebas con un mayor número de cuentas Ethereum que nos permitan estimar el rendimiento del sistema en un ambiente de producción óptimo.

BIBLIOGRAFÍA

[1] A. M. Bermúdez, *Study of evoting System using blockchain protocol*. PhD thesis, Universidad de Cataluña, 2016.

[2] V. M. Baldeón Coronel and J. F. Zambrano Hidalgo, *Implementaciòn de un prototipo de una red descentralizada blockchain para el voto electrónico en la Universidad De Guayaquil*. PhD thesis, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas …, 2018.

[3] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security analysis of the estonian internet voting system," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 703–715, 2014.

[4] J. D. Neira Gallo, *Estudio de factibilidad de un sistema de voto electrónico basado en la tecnología Blockchain para los procesos electorales de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil.* PhD thesis, Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de …, 2019.

[5] B. D. Agudelo Mogollón, B. A. Cruz López, D. G. Barajas Suarez, S. A. Chaparro Palacio, *et al.*, "Sistema de votación basado en blockchain: Pocket ballot chain," 2020.

[6] R. E. C. López, Y. L. M. Ramos, and J. A. M. Ortega, "Blockchain y su impacto en la economía: Sector banca, salud, internet of things, económica y voto electrónico.," *Revista Centroamericana de Administración Pública*, no. 77, pp. 23–31, 2019.

[7] W. Zhang, Y. Yuan, Y. Hu, S. Huang, S. Cao, A. Chopra, and S. Huang, "A privacy-preserving voting protocol on blockchain," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp. 401–408, IEEE, 2018.

[8] B. Y. Navarro, “Blockchain y sus aplicaciones,” *Recuperado de http://jeuazarru. com/wpcontent/uploads/2017/11/Blockchain. pdf*, 2017.

[9] R. Bulut, A. Kantarcı, S. Keskin, and Ş. Bahtiyar, “Blockchain-based electronic voting system for elections in turkey,” in *2019 4th International Conference on Computer Science and Engineering (UBMK)*, pp. 183–188, IEEE, 2019.

[10] F. D. Giraldo, M. C. Barbosa, and C. E. Gamboa, “Electronic voting using blockchain and smart contracts: Proof of concept,” *IEEE Latin America Transactions*, vol. 100, no. 1e, 2020.

[11] K. Patidar and S. Jain, “Decentralized e-voting portal using blockchain,” in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–4, IEEE, 2019.

[12] J. L. G. Sánchez, “La seguridad en la red,” *Informática y derecho: Revista iberoamericana de derecho informático*, no. 34, pp. 117–146, 2002.

[13] R. J. P. Zurdo, “«blockchain»: la descentralización del poder y su aplicación en la defensa,” *bie3: Boletín IEEE*, no. 10, pp. 885–904, 2018.

[14] J. S. Moreno Peláez *et al.*, “Blockchain por la educación,” B.S. thesis, Uniandes.

[15] H. Acuña, “Estudio sobre bitcoin y tecnología blockchain,” *Universidad de los Andes*, 2017.

APÉNDICES

.1 Manual de Usuario

.1.1 Proceso para crear una Elección

Los pasos para desplegar una elección son los siguientes:

1. La entidad electoral ingresa su cuenta Ethereum válida y el nombre de la elección como muestra la figura 1.

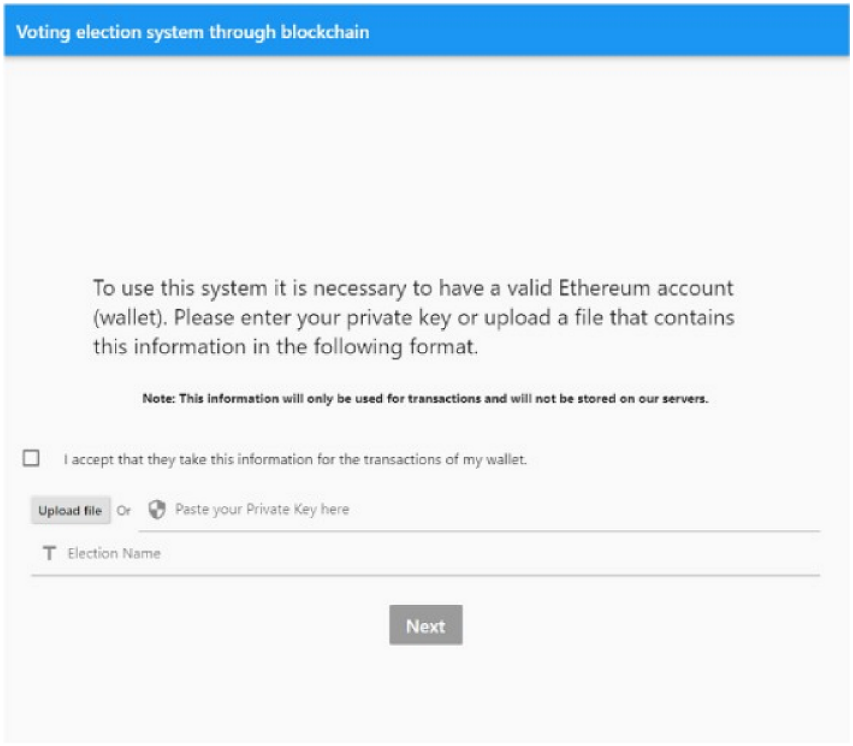

Figura 1: Crear elección: Paso 1

2. Una vez creada la elección se procede a incluir los candidatos que participaran en la misma como muestra la figura 2.

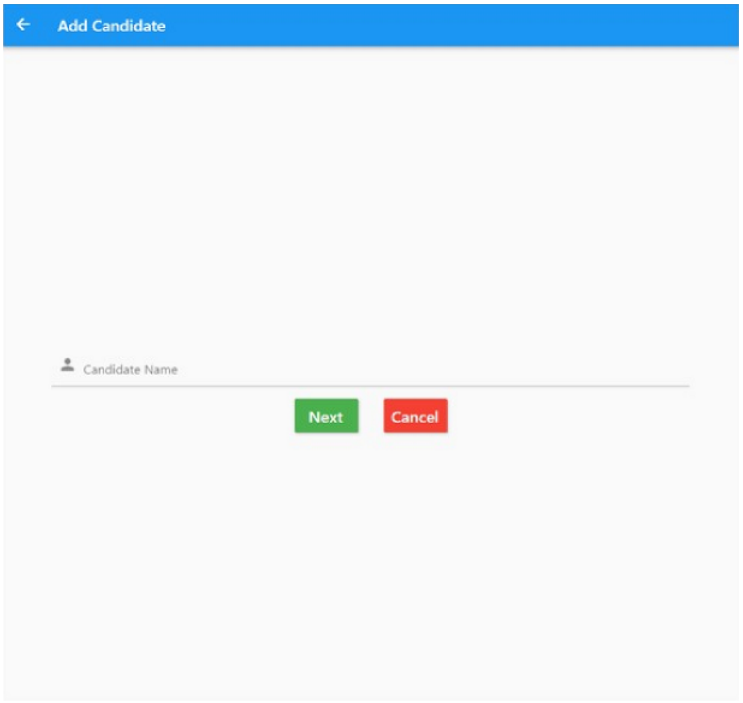

Figura 2: Crear elección: Paso 2

3. Luego se procede a ingresar las cuentas Ethereum de todos los votantes que van a participar en la elección como muestra la figura 3.

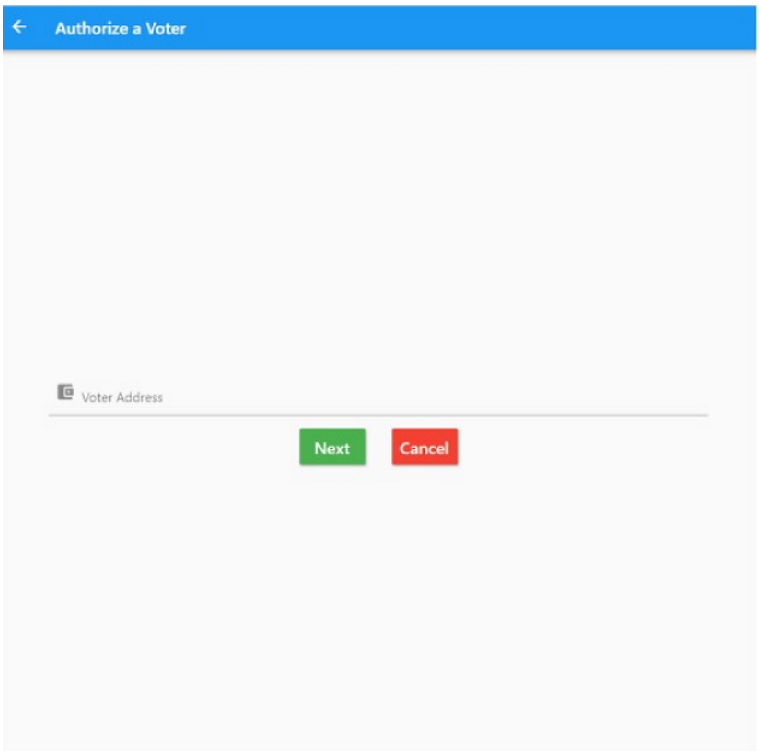

Figura 3: Crear elección: Paso 3

4. Finalmente se muestra una ventana con los candidatos ingresados y los votos

contabilizados como muestra la figura 4

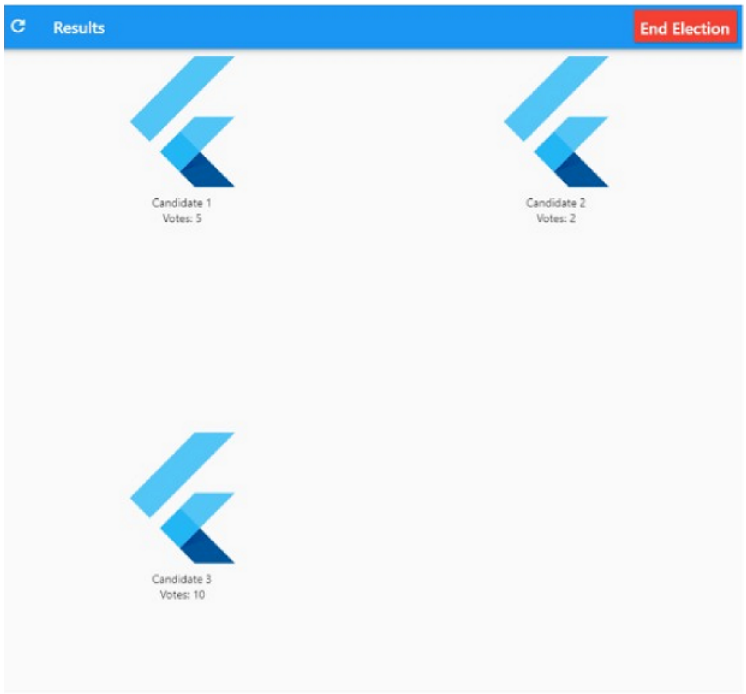

Figura 4: Crear elección: Paso 4

.1.2 Proceso para emitir un voto

Los pasos para realizar la votación son los siguientes:

1. El usuario ingresa el correo y clave proporcionada por la entidad electoral como muestra la figura 5.

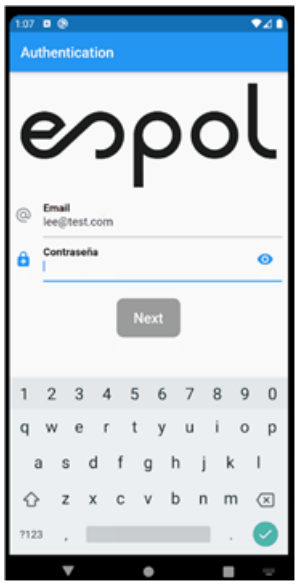

Figura 5: Emitir voto: Paso 1

2. Una vez que el usuario paso el proceso de autenticación se le muestran los candidatos a elegir, incluyendo nulos y blancos como muestra la figura 6.

Figura 6: Emitir voto: Paso 2

3. Cuando el usuario elige un candidato y presiona el boton Votar se le muestra un mensaje de confirmación de la opción elegida como muestra la figura 7.

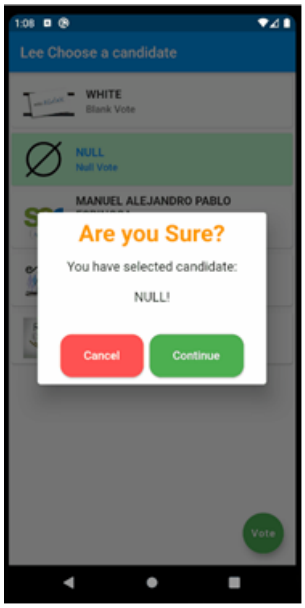

Figura 7: Emitir voto: Paso 3

4. Finalmente cuando el usuario confirma su voto accede a la ventana que se muestra en la figura 8 donde puede solo por unica vez ver los resultados de la elección hasta el momento de emitir su voto.

Figura 8: Emitir voto: Paso 4

.1.3 Escenario 1: Creacion exitosa de una elección

Dado que la entidad electoral ingresa correctamente su cuenta Ethereum y le da nombre a la elección se le muestra la ventana de la figura 9 en la que se le indica que la creación fue exitosa.

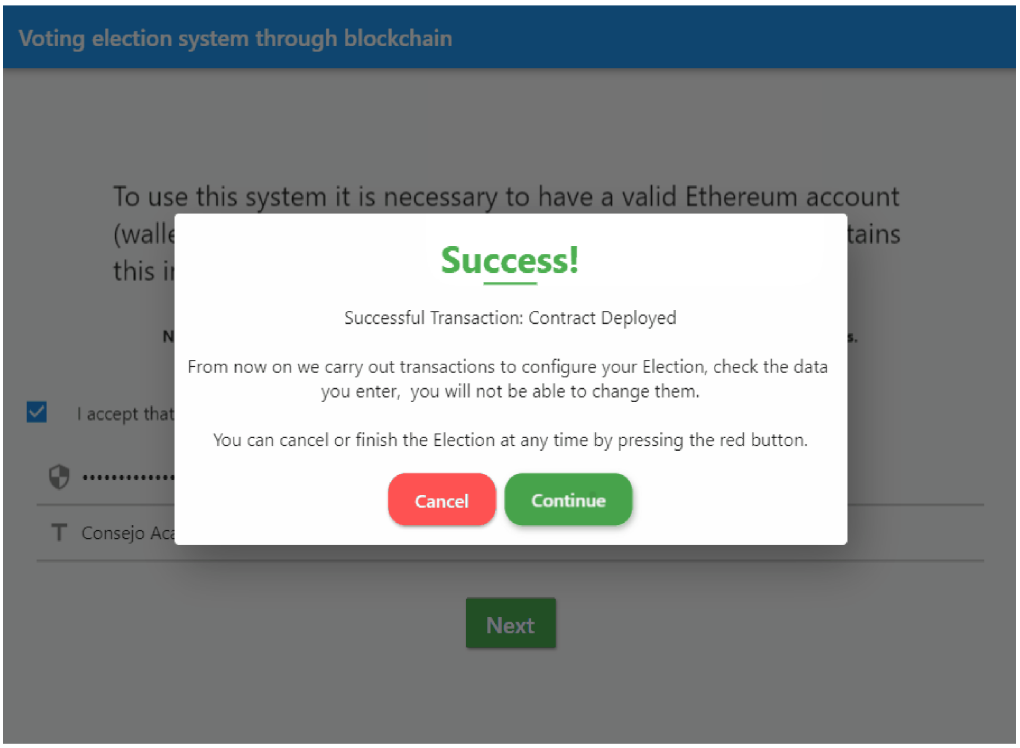

Figura 9: Creación exitosa de un elección

.1.4 Escenario 2: Usuario no autenticado

Este escenario se da cuando el votante ingresa incorrectamente su correo o contraseña, se entiende que no puede pasar el proceso de autenticación por ese motivo se le muestra un mensaje como el mostrado en la figura 10.

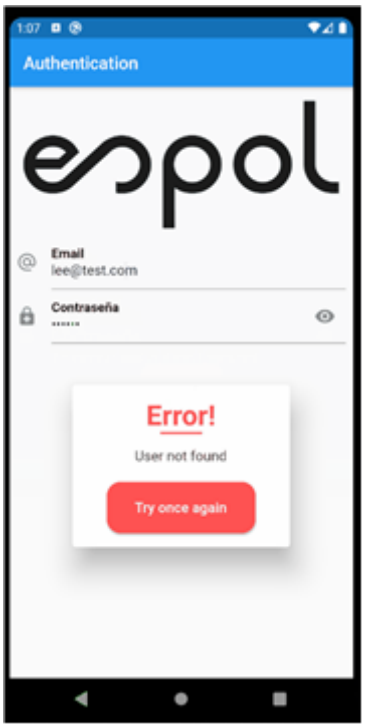

Figura 10: Mensaje de autenticación fallida