Recibido: 5 de mayo 2019 Aceptado: 28 de junio 2019

Modelo y sistema de votación electrónica aplicando la tecnología de cadena de bloques.

Model and electronic voting system applying Blockchain technology.

Gabriel Alejandro Lucuy, Sergio Andres Köller Vargas & Yanina Galaburda

Departamento de Ciencias Exactas e Ingeniería, Universidad Católica Boliviana "San Pablo", Calle M. Márquez esquina Parque Jorge Trigo Andia, Cochabamba, Bolivia

gabolucuy@hotmail.com

Resumen: Durante los últimos años se han implementado diferentes mecanismos para asegurar los requerimientos necesarios de un proceso electoral: libertad, equidad, franqueza, secreto y democracia. Existen procesos electorales tradicionales de votación física y procesos de votación electrónica que utilizan herramientas tecnológicas. Lamentablemente, los procedimientos aplicados no aseguran el cumplimiento de estos requerimientos en su totalidad, por lo cual la integridad de la información o la lucha contra el fraude se podría ver afectada.

Este artículo presenta un modelo de votación electrónica que integra aspectos del modelo tradicional, la tecnología Blockchain y la infraestructura transaccional de la moneda criptográfica Bitcoin, para implementar una votación descentralizada y anónima, asegurando la integridad de los datos ante cualquier posible dificultad que pueda surgir. Así mismo, este artículo presenta una implementación del modelo aplicado a los distintos procesos electorales que Bolivia tiene y un caso de estudio para la evaluación de la implementación del modelo.

Palabras clave: Blockchain, Bitcoin, Votación electrónica, Proceso electoral, Bolivia.

Abstract: For the past years, different mechanisms have been implemented to ensure the necessary requirements of an electoral process: freedom, fairness, openness, secrecy and democracy. There are traditional electoral processes and electronic voting processes that use technological tools. Unfortunately, the procedures applied do not ensure the accomplishments of these requirements in their absoluteness, so the integrity of the information or the fight against fraud could be affected.

This article presents an electronic voting model that integrates aspects of the traditional model, the Blockchain technology and the transactional infrastructure of Bitcoin cryptographic currency, to implement a decentralized and anonymous vote, ensuring the integrity of the data before any possible difficulty that may arise. Likewise, this article presents an implementation of the model applied to the different electoral processes that Bolivia has and a study case to evaluate the implementation of the model.

Key words: Blockchain, Bitcoin, Electronic voting, Electoral process, Bolivia.

1 Introducción

Hoy en día la mayoría de los países del mundo han optado por una forma de gobierno basada en la democracia, en la cual el poder es ejercido por el pueblo mediante mecanismos legales de participación para la toma de decisiones políticas. Cada país ha implementado modelos electorales propios de acuerdo a sus necesidades y situaciones propias. Sin embargo, todos tienen el mismo objetivo: asegurar un proceso transparente, seguro y confiable.

El avance en las tecnologías de información y comunicación juegan un papel importante en la evolución de los procesos electorales. Desde la década del 60 algunos países están implementando mecanismos y sistemas que permiten la votación electrónica, con el fin de mejorar la seguridad y confiablidad de una votación. Sin embargo, estos sistemas no pueden asegurar un proceso electoral totalmente seguro y confiable ante posibles ataques informáticos [25][26][27][28].

Este artículo describe un modelo e implementación de un sistema de votación electrónica[1] que aplica la tecnología de cadena de bloques capaz de soportar los distintos procesos electorales que Bolivia tiene.

2 Votación

2.1 Votación Tradicional

Actualmente en Bolivia se utiliza un proceso electoral manual y tradicional. Este consiste en una serie de pasos que concluyen en la cuantificación de los votos para realizar una toma de decisión política.

El proceso de votación inicia con el empadronamiento cuyo objetivo es inscribir a los ciudadanos para que tengan la oportunidad de ejercer su derecho al voto y estos sean asignados a los puntos donde podrán emitir su voto. El día de la votación el ciudadano recibe la papeleta de sufragio con previa verificación de que esta no tiene ninguna marca, a continuación, el ciudadano registra su voto y deposita su papeleta en el ánfora autorizada.

[1] Código fuente con su respectiva documentación se encuentra disponible en: https://gitlab.com/gabolucuy/Sistema_en_linea.git

Una vez concluido el proceso de votación, se inicia el proceso de conteo y escrutinio de los votos según la instancia encargada correspondiente.

Al contar con todos los resultados se procede a trasmitir los resultados finales.

2.2 Votación electrónica

Las tecnologías de información y comunicación ofrecen alternativas ante la necesidad de buscar procesos electorales más seguros y confiables dando lugar al uso de sistemas de votación electrónicos.

Los sistemas de votación electrónica se dividen en dos [1]:

- *E-Voting:* consiste en puntos de votación controlados por encargados, uso de máquinas electrónicas y posible uso de redes privadas.
- *Remote E-Voting*: consiste en la posibilidad de votar desde cualquier lugar mediante internet y servidores distribuidos.

Ambos proveen diferentes soluciones para aportar al proceso electoral siendo el más utilizado el primero [1].

2.3 Problemática

Ambas formas de votación presentan diferentes problemas descritos a continuación:

- Los procesos de conteo y escrutinio de votos conllevan altos costos económicos y requieren de mucho tiempo.
- En varias oportunidades se han denunciado fraudes electorales en los diferentes pasos del proceso electoral lo cual atenta contra la democracia y ocasiona desconfianza de la ciudadanía.
- La aplicación de procesos manuales genera la posibilidad de errores humanos.
- Un proceso electoral centralizado por entidades autónomas ocasiona desconfianza entre los ciudadanos.
- En los sistemas de voto electrónico remoto por internet no se puede asegurar la identidad de la persona que está realizando el voto.
- Los sistemas que hacen uso de redes privadas para intercambiar la información, son vulnerables ante un ataque informático poniendo en riesgo la integridad de los votos.
- En los sistemas de votación centralizada, cualquier persona con acceso podría adulterar los resultados del proceso electoral.

3 Blockchain

Para mitigar vulnerabilidades en cuanto a la integridad de la información y lograr la descentralización de datos, en el año 2008 nació el concepto de cadena de bloques o *Blockchain* como parte de la moneda criptográfica *Bitcoin* [2].

3.1 Generalidades e historia de Blockchain

Blockchain es, en esencia, una base de datos distribuida o un libro mayor público de todas las transacciones o eventos digitales que han sido ejecutados y compartidos entre las partes participantes. Cada transacción se verifica por consenso de la mayoría de los participantes en el sistema y, una vez ejecutada la transacción, su información nunca podrá ser borrada o alterada [3].

Existen diferentes formas de gestionar la administración y el almacenamiento de datos en un sistema. En un sistema centralizado un solo nodo es el encargado de almacenar la información, en un sistema descentralizado son varios nodos que la almacenan, mientras que en un sistema distribuido como Blockchain todos los involucrados tienen acceso y una copia de toda la información. Se puede ver el ejemplo gráfico en la Figura 1:.

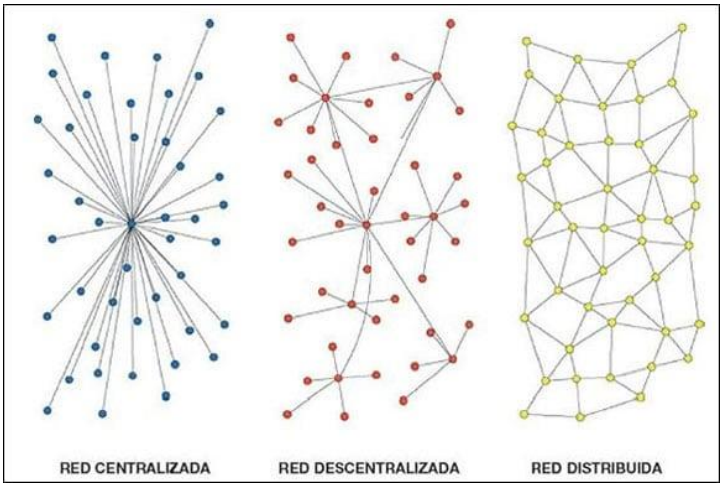

Figura 1: Tipos de redes [4].

La idea de una cadena de bloques se empezó a trabajar desde el año 1991 por Stuart Haber y W. Scott Stornetta, seguido por publicaciones el año 1996 por Ross J Anderson y en 1998 por Bruce Schneier y John Kelsey. El año 2000 Stefan Konst publicó una teoría general sobre la implementación de una cadena de bloques y sus posibles implementaciones [5].

La primera Blockchain fue conceptualizada por Satoshi Nakamoto, creador de Bitcoin, e implementada en la moneda criptográfica Bitcoin el año 2008. Este dato no es un dato confirmado ya que Satoshi Nakamoto es un seudónimo de lo que posiblemente podría ser más de una persona [6].

Blockchain es la solución para realizar transacciones de bienes entre dos entidades sin la necesidad de una tercera, cuyo objetivo se centra en la seguridad y privacidad de una transacción y su información [23].

3.2 Tipos de Blockchain

Existen tres tipos de Blockchain [12]:

- Las Blockchain públicas, como Bitcoin o Ethereum, son accesibles para cualquier usuario en el mundo con un computador y acceso a internet. En este tipo de Blockchain todo el mundo tiene derecho de enviar una transacción, de participar en el proceso de consenso o de tener lectura a toda la información.
- Las Blockchain privadas, donde el acceso solo se puede dar existiendo una invitación de por medio, o algún tipo de autenticación del nodo. Las acciones de la Blockchain solo podrán ser realizadas por los denominados nodos de confianza.
- Por último, se cuenta con las Blockchain híbridas o Blockchain con permisos, las cuales son una combinación de las previamente mencionadas. En una Blockchain hibrida se puede combinar aspectos de ambos tipos de Blockchain para contar con una lista de nodos con ciertos permisos y con una visibilidad a la información pública [36].

3.3 Multichain

Multichain es una plataforma para la creación y el uso de Blockchains híbridas y privadas. Tiene el objetivo de construir Blockchains en el sector institucional otorgando privacidad y el control requerido en un paquete de fácil uso. Como el núcleo de Bitcoin, esta plataforma es aceptada en cualquier sistema operativo [7].

MultiChain es una plataforma que ofrece una serie de comandos API que permiten diseñar, implementar y operar registros distribuidos del tipo Blockchain de manera rápida y sencilla. Cada comando API tiene que ser ejecutado en un intérprete

de comandos[2]. Asimismo, multichain es compatible con una variedad de populares lenguajes de programación como *Phyton*, C#, *Javascript*, *PHP*, *Ruby,* entre otros [8].

4 Modelo de Votación Basado en Blockchain

4.1 Generalidades del modelo

Debido a las falencias que presentan los procesos electorales remotos y los sistemas electorales tradicionales, se decidió proponer un modelo de votación electrónica que separe los procesos de autenticación del votante y la emisión de un voto, con el fin de promover un proceso electoral confiable, transparente y seguro.

El modelo propuesto tiene como objetivo brindar apoyo informático durante la gestión de un proceso electoral y durante los procesos de emisión, conteo y escrutinio de votos. Asimismo, se plantea el modelo para ser integrado en los procesos que se lleven a cabo durante el empadronamiento y autenticación del votante, ya que no brindaráapoyo informático en estos procesos.

En esencia, se propone manejar una votación como un intercambio de bienes (votos) entre los ciudadanos y los candidatos y que cada transacción sea almacenada en una Blockchain.

El modelo propuesto se explica en las siguientes subsecciones.

4.2 Actores

Durante un proceso electoral participarán los actores diferenciados por las tareas y permisos que tengan para llevar a cabo una votación exitosamente. Se dividió los actores en dos categorías, los actores informáticos y los actores humanos.

4.2.1 Actores informáticos

Los actores informáticos son todos los sistemas y elementos informáticos autónomos que forman parte la de ejecución del modelo propuesto y se explican a continuación.

[2] **Interprete de comandos.** Interfaz entre el usuario y el sistema operativo. Su función es la de leer la línea de comandos, interpretar su significado, llevar a cabo el comando y después devolver el resultado por medio de las salidas [24].

- Sistema de Emisión de Voto. Éste se encarga del proceso de emisión de votos. Se instala en todas las máquinas autorizadas para emitir un voto y trabaja en sincronía con la Blockchain y el Sistema en Línea.
- Vocero en línea. Este se encarga de comunicar los resultados parciales y totales de la votación junto con los parámetros de votación. Reporta los resultados parciales y totales por mesa, sector, recinto y departamento además del resultado final. Se comunica directamente con el Sistema en Línea para obtener los datos.
- Sistema en Línea. Este sistema se encarga del trabajo de todos los encargados de la votación y su participación dentro del sistema. Utilizando este sistema se pueden configurar todos los parámetros de una votación. Este sistema será el encargado de identificar a todos los encargados y proveerles las herramientas informáticas necesarias para desempeñar parte de su papel durante el proceso electoral. Se conecta directamente con la Blockchain para el registro de los candidatos y la obtención de resultados.
- Blockchain. Este sistema se encarga de almacenar todos los votos, junto con la información respectiva a su proveniencia.

4.2.2 Actores Humanos

Los actores humanos son los actores necesarios para la ejecución del modelo propuesto y se explican a continuación.

- Encargado de la votación. Se encarga de establecer los parámetros necesarios para una votación, crear los departamentos, gestionar un proceso electoral y asignar las cuentas generadas por el Sistema en Línea a los encargados de departamento.
- Encargado de departamento. Éste se encarga de crear los sectores de su departamento y asignar las cuentas generadas por el Sistema en Línea a los encargados de sector.
- Encargado de sector. Éste se encarga de crear los recintos de su sector y asignar las cuentas generadas por el Sistema en Línea a los encargados de recinto.
- Encargado de recinto. Éste se encarga de crear las mesas de su recinto y asignar las cuentas generadas por el Sistema en Línea a los encargados de mesa.
- Encargado de mesa. Éste se encarga de habilitar la máquina donde se emitirá el voto para cada uno de los votantes. También se encarga de informar el estado de la mesa y acudir al votante en cualquier dificultad.

- Ciudadano que aporta. Éste instalará el *script* de nodo de apoyo para integrar su computador como nodo de la Blockchain.
- Votante. Éste es el individuo con derecho a voto el cual hace uso del Sistema de Emisión de Voto para llevar a cabo su voto y así registrar su decisión.
- Sociedad. Este actor puede recibir la información resumida para ver la decisión tomada por todos los votantes al finalizar el proceso electoral.

En la Figura 2: se describe la relación entre los actores humanos e informáticos.

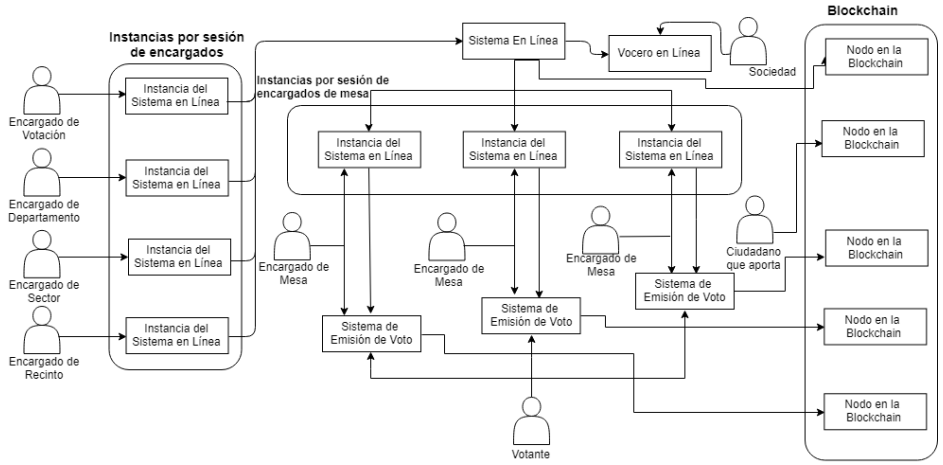

Figura 2: Relación entre actores del modelo.

4.3 Etapas de una votación

El modelo plantea dividir un proceso electoral en tres etapas:

- Previo a la votación. Durante esta etapa se establecen todos los parámetros necesarios para llevar la votación. Se definen también todos los departamentos, sectores, recintos y mesas donde se emiten los votos y se procede a instalar todo lo necesario en las máquinas que serán utilizadas. Se integran también todos los nodos de apoyo.
- Durante la votación. Durante esta etapa se emiten todos los votos de los ciudadanos con derecho a votar en las mesas donde se encuentran asignados. Se liberan resultados parciales de las mesas finalizadas, de los recintos finalizados, de los sectores y los departamentos. Al finalizar este proceso se presentan los resultados finales.
- Finalizando la votación. Durante esta etapa se deshabilitan los actores informáticos.

4.4 Flujo para registrar un voto en la Blockchain

Como cada voto es un bien que será enviado de un ciudadano a un candidato en específico, se propone el siguiente flujo para registrar satisfactoriamente un voto en la Blockchain:

- Paso 1. Crear una billetera electrónica para cada votante, únicamente con un voto (un "coin" en la billetera del votante) para ser transferido.
- Paso 2. El ciudadano según su preferencia escoge a un candidato.
- Paso 3. El voto será transferido a la billetera electrónica del candidato y dicha transacción será almacenada en la Blockchain.

En la Figura 3: se muestra la relación entre los actores humanos e informáticos y las tareas que se llevan a cabo para registrar un voto en la Blockchain.

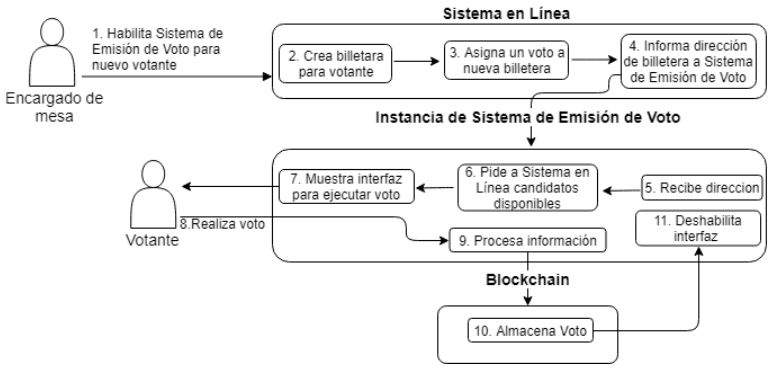

Figura 3: Flujo para registrar un voto en la Blockchain.

5 Implementación y adaptación del modelo para Bolivia

5.1 Requerimientos de los procesos electorales

En Bolivia, según la Ley del Régimen Electoral, existen diferentes procesos electorales que hacen uso del sufragio universal[3], según el tipo de decisión que se necesite llevar a cabo [10]:

- Referendos.

[3] **Sufragio universal.** Consiste en el derecho de la población adulta de un estado a ejercer su voto [11].

- Elecciones Generales.
- Elecciones Municipales.
- Elecciones departamentales.
- Elecciones judiciales.

5.2 Adaptación del modelo

Con el objetivo de crear un modelo de votación que sea capaz de funcionar bajo cualquier proceso electoral que Bolivia presenta, se propuso un modelo de datos para ser implementado junto con el Sistema en Línea.

Este modelo propone descomponer un proceso electoral por partes, creando el proceso electoral como tal hasta agregar candidato por candidato. En la Tabla 1 se definen las clases involucradas, su propósito y su semejanza con un proceso electoral.

Tabla 1. Modelo de datos para procesos electorales bolivianos.

Nombre de la clase	Propósito	Ejemplo
ProcesoElectoral	La clase "Proceso electoral" tiene como objetivo crear al proceso electoral como tal, como primer paso.	- Elecciones generales. - Elecciones. - Referéndums.
Boleta	La clase "Boleta" tiene como objetivo crear una papeleta que puede ser usada para todos los departamentos de Bolivia o crear una por departamento según el caso.	- Elecciones departamentales Cochabamba. - Elecciones generales (Para toda Bolivia).
BoletaItem	La clase "Boleta Item" tiene como objetivo crear los diferentes tipos de candidatos que una Boleta pueda tener.	- Candidatos a presidencia. - Candidatos a vicepresidencia. -Candidatos a gobernación.
OpcionCandidato	La clase "Opcion candidato" tiene como objetivo agregar los candidatos que conforman una Boleta Item	- Candidato 1. - Candidato 2.
OpcionReferendum	La clase "Opcion Referendum" tiene como objetivo agregar las preguntas que conforman una Boleta Item.	- Pregunta 1. - Pregunta 2.

5.3 Rendimiento en ambiente de producción

El Sistema en Línea fue instalado en un servidor virtual privado de la plataforma "Digital Ocean", con las siguientes características: 1 *CPU* [4], 1 *Gb* de memoria *RAM* [5] y 20 *Gb* de almacenamiento.

El Sistema de Emisión de Voto fue planeado a ser instalado en 27 computadoras, con el objetivo de simular 27 mesas electorales. Sin embargo, al instalar el sistema en la novena computadora el sistema no pudo funcionar correctamente. Por tanto, se procedió con un análisis de las causas del problema detectado y se ha determinado lo siguiente:

Considerando que el Sistema de Emisión de voto actúa como nodo en la *Blockchain,* este necesita permisos otorgados únicamente por el Sistema en Línea para poder realizar la emisión de un voto. Cada una de estas solicitudes del Sistema de Emisión de Voto requiere que el servidor donde se encuentra el Sistema en Línea ejecute un subproceso a fin de otorgar los permisos requeridos en la *Blockchain.*

Cada subproceso consume memoria *RAM* del servidor virtual, el cual se veía limitado en cuanto a recursos disponibles llegando a su máxima capacidad sin poder permitir más conexiones simultáneas.

Según las primeras pruebas, el servidor logró establecer satisfactoriamente una conexión simultánea de hasta ocho conexiones. Asimismo, el siguiente paso fue determinar cuanta memoria utiliza cada subproceso.

Según la documentación de Phusion Passenger6 el número máximo de procesos que un servidor puede atender simultáneamente está dado de acuerdo a la cantidad de CPUs, memoria RAM y memoria requerida por cada subproceso que el servidor tenga a disposición. Este número se calcula a partir de una pequeña fórmula matemática:

[4] ***CPU*.** Unidad central de procesamiento o llamado procesador, es el componente en un ordenador que interpreta las instrucciones y procesa los datos contenidos en un programa.
[5] ***RAM*.** Memoria de acceso aleatorio, es donde el computador guarda los datos que utilizando ese momento. Es considerado temporal porque solo guarda los datos mientras la computadora esté encendida.
[6] **Phusion Passenger.** Servidor de aplicaciones web utilizado para instalar el Sistema en Línea en un ambiente de producción.

numero_maximo_de_procesos = (memoria_disponible * 0.75) / memoria_requerida_por_proceso

ec. 1

Según la información obtenida se pudo crear 3 escenarios diferentes de ambientes de producción, los dos primeros fueron probados y analizados y el último escenario es una extrapolación de los dos primeros para poder llevar a cabo una votación a nivel nacional.

- **Escenario 1:** Está compuesto por el servidor virtual detallado al principio de esta subsección y 9 computadoras en las cuales se instaló el Sistema de Emisión de Voto. En este escenario la memoria *RAM* disponible en el servidor es ocupada totalmente, permitiendo de esta manera poder trabajar solo con 9 instancias del Sistema de Emisión de Voto.
- De acuerdo a la ec. 1, se puede determinar que cada subproceso en cada instancia del Sistema de Emisión de voto consume alrededor de 96 MB de memoria.
- **Escenario 2:** El objetivo de este escenario es el de optimizar los recursos del servidor virtual con el fin de que éste pueda soportar mayor número de instancias del Sistema de Emisión de Voto.
- Para llevar a cabo esta tarea, se creó un SWAP. Un *SWAP* es un espacio de intercambio que utiliza el disco duro en lugar de la memoria RAM para almacenar datos temporalmente [13]. El tamaño máximo recomendable de un *SWAP* es el doble de espacio de memoria RAM disponible [14]. De esta manera el servidor llegó a contar con 3*Gb* de memoria RAM disponibles, pudiendo triplicar el número de instancias del Sistema de Emisión de Voto a 27, sin la necesidad de requerir más recursos de los ya disponibles en el servidor.
- **Escenario 3:** El objetivo de este escenario es el de extrapolar los recursos mínimos que serían necesarios para llevar a cabo una votación a gran escala a nivel nacional.

  Según informes de la última elección general que se llevó a cabo en Bolivia el año 2014, se necesitó un total de 24,509 mesas distribuidas en todo el país [15], esto significa que el sistema de Emisión de Voto debería ser instalado en este número de computadoras. Por consiguiente, el Sistema en Línea deberá manejar 24,509 instancias del Sistema de Emisión de Voto.

  Acorde a los cálculos obtenidos del escenario 1, para cubrir todas las conexiones necesarias se requerirá de un servidor con 3068.5 *Gb* de memoria *RAM*. Un servidor con estas características no es viable.

La solución propuesta para implementar los sistemas en producción es usar 6 servidores distribuidos de 256 Gb de memoria *RAM* cada uno, además de realizar un *SWAP* en cada servidor para aumentar la cantidad de memoria *RAM* disponible de este y así cada servidor podría manejar mayor cantidad de conexiones simultáneas.

6 Estudio de usuarios.

En esta sección se describe un estudio de usuarios realizado en la Universidad Católica Boliviana "San Pablo" – Regional Cochabamba para comprobar el rendimiento[7] y la usabilidad de los sistemas implementados en un ambiente de producción.

6.1 Participantes

Al estudio de usuarios asistieron un total de 32 personas, este grupo fue conformado por estudiantes de diversas carreras y semestres, docentes de la carrera de Ingeniería de Sistemas y personal administrativo de la universidad.

6.2 Tareas y sesiones de trabajo

Cada sesión de trabajo consistió en que cada participante simule ser un ciudadano que está participando en un proceso electoral. Las tareas involucradas fueron las siguientes

- **Explicación.** A cada participante se le dio una pequeña introducción sobre Blockchain y sus beneficios y por último se dio una breve explicación sobre el modelo propuesto en este artículo.
- **Realizar Voto.** A cada participante se le habilitó una máquina con el Sistema de Emisión de Voto instalado, no se dio una explicación de cómo usar este sistema, con el objetivo de obtener retroalimentación en cuanto a la usabilidad de este sistema.
- **Retroalimentación.** Una vez concluido el voto de cada participante, se le pidió que llene una encuesta. Las preguntas realizadas se exponen en la Tabla 2.

[7] **Rendimiento.** El rendimiento de un sistema informático depende de cómo éste utiliza y asigna sus recursos. Se debe tener una idea clara sobre lo que se espera y también se debe poder reconocer los problemas cuando se producen [12].

Tabla 2. Preguntas a los participantes.

Pregunta	Razón Fundamental
• ¿Tuviste algún problema al utilizar el sistema? • En caso de que tuviste algún problema. ¿Cuál fue?	Identificar problemas o errores durante el proceso de votación de un participante.
• ¿La interfaz fue clara y fácil de usar? • En caso de no ser clara. ¿Qué fue lo que te confundió?	Identificar si el participante pudo usar el sistema sin problemas.
• En base a tu experiencia ¿Consideras que existe alguna • característica del sistema tradicional que no tuviste con • el sistema electrónico? • ¿Qué consideras que faltaría?	Tratar de que el modelo planteado sea lo más próximo al sistema tradicional que los participantes conocen y ya utilizaron antes.
• ¿Te gustaría utilizar en futuro el sistema electrónico • planteado para los distintos procesos electorales de Bolivia? • En caso de no estar seguro de utilizar un sistema electrónico. • ¿Cuál sería tu mayor inseguridad? • ¿Qué opinas del sistema tradicional de votación • actual de Bolivia?	Entender la opinión que los participantes tienen sobre el modelo planteado y sobre el modelo de votación tradicional actualmente usado en Bolivia.

6.3 Resultados y Discusión.

Con la implementación del sistema desarrollado sobre la base del modelo diseñado, se ha evidenciado lo siguiente:

- Usabilidad. Ninguno de los 32 participantes tuvo problemas o dificultades para llevar a cabo su voto de manera satisfactoria. Sin la necesidad de una explicación previa sobre cómo funciona el Sistema de Emisión de Voto, cada participante pudo por sí mismo interactuar con dicho sistema para completar su tarea. Por tanto, la verificación realizada permitió comprobar que en caso de implantar el sistema a nivel nacional, los ciudadanos no requerirían de una capacitación extensa, tan solo una guía resumida de pasos a seguir.

- Rendimiento. Durante todo el estudio se monitoreó el estado de los recursos del servidor virtual en el cual se encontraba instalado el Sistema en Línea. Hasta que el estudio finalizó, el servidor trabajó con normalidad sin presentar problemas en el manejo de recursos y el Sistema en Línea no presentó errores durante su ejecución permitiendo de esta manera concluir el proceso de elección de candidatos como un caso de estudio.

- Retroalimentación. Parte de las preguntas de la encuesta tenían como objetivo obtener retroalimentación sobre posibles mejoras que podrían implementarse al Sistema de Emisión de Voto, con el objetivo de asemejar lo más posible el proceso de registro de un voto presentado en este trabajo al modelo de votación actual de Bolivia. Se logró obtener mejoras que posteriormente fueron implementadas gracias a su relevancia en el objetivo de presentar una interfaz clara e intuitiva.

7 Validación del modelo

7.1 Validación de condiciones para voto electrónico seguro

En la Tabla 3 se describen las condiciones constitucionales y los principios para llevar a cabo un voto electrónico seguro [16] [17] [18] [19]. Asimismo se describe la manera en la que modelo diseñado e implementado en este trabajo valida las condiciones mencionadas.

Tabla 3. Tabla de validación de condiciones para voto electrónico seguro.

Descripción de la condición	Validación del modelo
Los equipos y el *software* deben ser diseñados a prueba de fraude.	La aplicación de tecnología Blockchain previene el fraude considerando mecanismos que garantizan la integridad de información y la confidencialidad de la identidad del votante.
El código fuente debe estar disponible para inspección en cualquier momento, junto a su documentación correspondiente.	El presente modelo junto al sistema implementado se encuentran documentados en la presente investigación. Implementaciones futuras para su uso en un ambiente real deberían ser de código abierto y con una documentación exhaustiva detallando todas las partes del sistema.
Es necesario que todos los niveles del sistema a nivel de código puedan ser accedidos por cualquier individuo.	Los niveles del sistema propuesto en el modelo pueden ser accedidos por cualquier persona para las revisiones pertinentes. Al momento de empezar con las etapas respectivas, estos accesos solo se darán a las personas con los permisos necesarios.
Es recomendable el uso de redundancia.	El modelo no restringe el uso de un sistema o modelo paralelo para el trabajo de redundancia.
Es necesario que la documentación pertinente al sistema sea clara y contenga la información necesaria y completa de cada aspecto del proceso.	El modelo se encuentra documentado en la presente investigación, tanto como la ingeniería respectiva al prototipo. Para implementaciones en ambiente real es necesario hacer obligatorio este aspecto.

Descripción de la condición	Validación del modelo
El diseño, implementación y mantenimiento deben minimizar las posibilidades de algún mal funcionamiento.	El modelo está diseñado evitando cualquier tipo de falla. En implementaciones en ambiente real es necesario realizar auditorías constantes para ver el estado del sistema.
Los sistemas centralizados pueden conducir al peligro de la manipulación de los datos por lo cual se compromete todo el proceso.	El modelo se implementa en un sistema descentralizado haciendo uso de la tecnología Blockchain.
Es necesario dejar evidencia física del voto para poder recontarlo y responder a reclamos o dudas.	El modelo no restringe el uso de este tipo de redundancia. Si se vela por la seguridad del proceso, sacrificando recursos, es posible emitir evidencia física de los votos para realizar reconteos y validar la información proveniente de la aplicación del modelo.
Los operadores internos del sistema deben asegurar que no se pueda ingresar al sistema por una puerta trasera o alguna contraseña alfanumérica. La autenticación para el ingreso al sistema debe ser sujeto al uso de mecanismos de identificación precisos de carácter biométricos.	El modelo no restringe la autenticación biométrica para los encargados. Se recomienda el uso de estos procesos de autenticación para implementaciones en ambiente real.
Todo sistema sufre de ser vulnerable, por lo cual es necesario realizar auditorías constantes y revisiones del sistema.	Para implementaciones en ambiente real es necesario que el sistema implementado en base al modelo, tenga revisiones y auditorias constantes.
Posteriormente a la votación, el sistema debe ser auditado nuevamente produciendo una evaluación integral de su operación.	Al finalizar la votación, un organismo independiente se deberá encargar de realizar una auditoría de las transacciones realizadas en el sistema durante el proceso de votación.
El sistema debe permitir imprimir en papel las operaciones realizadas para comprobar resultados en cualquier etapa del proceso.	El modelo planteado no restringe las impresiones en papel de todas las operaciones realizadas en cada etapa del proceso.

7.2 Validación de aplicabilidad de la infraestructura Bitcoin

En la Tabla 4 se describen las características principales de la infraestructura Bitcoin [20][21][22] y cómo éstas son aplicadas en el modelo diseñado.

Tabla 4. Aplicación de las características de la infraestructura Bitcoin en el modelo

Característica	Aplicación en el modelo
Es una infraestructura enfocada en la transacción de una moneda virtual.	Tanto como una moneda, la emisión de un voto puede ser interpretado como una transacción de un bien de valor. El modelo hace uso de transacciones para la emisión de los votos.
Es una infraestructura descentralizada.	Esta infraestructura permite que Bitcoin no sea regulada por ninguna entidad tercera, y que toda la información se maneje de manera descentralizada. El modelo destaca este principio debido a los beneficios directos en el trabajo de la confianza y la lucha contra el fraude.
Es imposible la falsificación o duplicación de las transacciones.	La implementación de la tecnología detrás de la infraestructura Bitcoin impide que las transacciones sean falsificadas o duplicadas. Este es un aspecto fundamental en una votación, ya que los votos no pueden sufrir de estos fraudes, por lo cual el modelo usa la tecnología.
Las transacciones son irreversibles.	Al igual que una transacción, un voto emitido no puede ser editado ni eliminado. El modelo utiliza la tecnología Blockchain para este cometido, al igual que la infraestructura Bitcoin.
Las transacciones se dan de manera anónima.	El usuario que emite una transacción solo hace uso de su llave pública, sin revelar ningún tipo de información personal. Debido al anonimato necesario en la emisión de un voto, el modelo hace uso del mismo paradigma.

7.3 Validación de solución a los problemas planteados

Finalmente, en la Tabla 5 se hace una demostración de la forma en que fueron solucionados problemas que presentan en la actualidad los sistemas de votación tradicionales (que aplican procedimientos manuales) y sistemas de voto electrónico.

Tabla 5. Validación de solución a los problemas planteados en los modelos de votación.

Problema	Validación del modelo
El proceso de conteo y escrutinio de votos, junto con la preparación de resultados para su transmisión conllevan altos costos económicos y requieren de mucho tiempo.	El modelo hace uso de las herramientas informáticas para automatizar en su totalidad el proceso de conteo, reconteo de votos y transmisión de resultados comprometiendo de manera positiva el uso de recursos económicos y humanos.
En varias oportunidades se han denunciado fraudes electorales en los diferentes	El hacer uso de un modelo de votación descentralizado, con procesos automatizados y una implementación validada por diferentes instituciones y todos los frentes

Problema	Validación del modelo
pasos del proceso electoral lo cual atenta contra la democracia y ocasiona desconfianza de la ciudadanía.	candidatos, afianza la confianza de los ciudadanos con el proceso electoral y disminuye la posibilidad de fraude.
Al contar con procesos manuales se da la posibilidad de errores humanos.	El automatizar los procesos críticos del proceso electoral, conteo y reconteo de votos, evitamos la posibilidad de desacreditar el resultado por un error humano.
El contar con el proceso electoral centralizado por entidades autónomas ocasiona desconfianza entre los ciudadanos	El modelo propuesto es totalmente descentralizado. El uso de la tecnología Blockchain permite que la información no pase por filtros en ninguna de sus etapas. Los votos son registrados, sin posibilidad de cambio, desde su emisión.
En los sistemas de voto electrónico remoto por internet no se puede asegurar que la persona que está votando sea quien dice ser.	Por esta razón es que el modelo propuesto combina aspectos del voto tradicional, junto con el voto electrónico. Al hacer uso de un proceso tradicional en el registro del votante, tanto como su autenticación estamos evitando el principal problema en el voto electrónico remoto. Por otro lado, el modelo está pensado para que en esta primera etapa de registro y autenticación, pueden ser utilizados otros tipos de modelos y sistemas para su ejecución, ya que se asegura que no exista ninguna relación con la emisión del voto y lo involucrado a este. Una disociación de ambos procesos nos permite asegurar la confidencialidad del voto.
En variados sistemas de voto electrónico no se puede asegurar la integridad de los votos.	La integridad de la información es la razón principal para el uso de la tecnología Blockchain. Esta tecnología nos permite asegurar la integridad de cada uno de los votos desde el momento de su emisión.
Los sistemas necesitan ser examinados por encargados de los partidos participantes o ser de código abierto para poder definirse como sistemas confiables, lo cual no siempre sucede.	Este problema marca una dirección para la posible aplicación del modelo planteado. La investigación tiene un carácter abierto. Una implementación debería ser examinada por instituciones y por expertos en los frentes candidatos de manera obligatoria.
En los sistemas que hacen uso de redes privadas para intercambiar la información no se puede asegurar la prevención ante un ataque informático.	Al ser cada computador donde se emite el voto un nodo de la cadena de bloques, este registra directamente el voto dentro de la Blockchain al momento de votar. Por otro lado, la tecnología utilizada asegura la propagación de la transacción de una manera segura. Un ataque informático no podría desacreditar la votación.
En los sistemas de votación centralizada cualquier persona con acceso podría adulterar los resultados del proceso electoral.	El modelo propuesto almacena su información de manera descentralizada gracias al uso de la tecnología Blockchain. Por esta razón ni las cuentas con más altos privilegios pueden realizar un cambio en la integridad de la información.

8 Conclusión

El análisis de la tecnología de cadena de bloques (Blockchain) y la infraestructura de la moneda criptográfica (Bitcoin) han permitido determinar los componentes esenciales para asegurar la integridad y disponibilidad de información relacionada con un proceso electoral.

A través del estudio de modelos de votación tradicional y votación electrónica se han establecido principios y requerimientos de un modelo de votación electrónica y se identificaron mecanismos que han permitido lograr el cumplimiento de los requerimientos en su totalidad coadyuvando a la lucha contra el fraude electoral.

Se ha diseñado el modelo de votación electrónica para una elección de gran envergadura integrando los aspectos de la infraestructura de moneda criptográfica Bitcoin y la tecnología Blockchain para implementar una votación descentralizada y anónima, asegurando la integridad de cada uno de los votos.

Asimismo, se ha implementado un sistema de votación electrónica capaz de soportar los diferentes procesos electorales que Bolivia tiene. El conjunto de sistemas desarrollados logró trabajar en sincronía para ofrecer las herramientas necesarias para gestionar un proceso electoral, emitir un voto y mostrar los resultados finales de un proceso electoral.

Referencias Bibliográficas

[1] Aceproject, "Electronic Voting". [En Línea]. Disponible en: http://aceproject.org/ace-en/focus/e-voting/types-of-e-voting

[2] BBVA, "De Alan Turing al 'ciberpunk': la historia de Blockchain". [En Línea]. Disponible en: https://www.bbva.com/es/historia-origen-blockchain-bitcoin/

[3] Berkeley University, "Blockchain Technology". [En Línea]. Disponible en: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

[4] Icommunity, "Redes centralizadas VS distribuidas". [En Línea]. Disponible en: https://icommunity.io/redes-centralizadas-vs-distribuidas/

[5] Vinay Gupta." A Brief History of Blockchain". [En Línea]. Disponible en: https://hbr.org/2017/02/a-brief-history-of-blockchain

[6] History of Bitcoin, "History of Bitcoin". [En Línea]. Disponible en: http://historyofbitcoin.org/

[7] Dr. Gideon Greenspan, "Multichain". [En Línea]. Disponible en: https://www.multichain.com/download/MultiChain-White-Paper.pdf

[8] Multichain. [En Línea]. Disponible en: https://www.multichain.com/developers/

[9] Órgano electoral Plurinacional. [En Línea]. Disponible en: https://www.oep.org.bo/wp-content/uploads/2017/01/habilitados_por_recinto.pdf

[10] Portal juridico Lexivox, "Ley del Régimen Electoral ". [En Línea]. Disponible en: https://www.lexivox.org/norms/BO-L-N26.xhtml

[11] EcuRed, "Sufragio Universal". [En Línea]. Disponible en; https://www.ecured.cu/Sufragio_universal

[12] Vitalik Buterin, "On public and private Blockchains". [En Línea]. Disponible en: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[13] Oracle, "Rendimiento y recursos del sistema". [En Línea]. Disponible en: https://docs.oracle.com/cd/E38897_01/html/E23086/spconcepts-19978.html

[14] Hipertextual. "Para qué sirve el Swap en Linux y cómo cambiarlo". [En Línea]. Disponible en: https://hipertextual.com/2015/09/swap-en-linux

[15] DigitalOcean, "How to Add Swap Space on Ubuntu 16.04". [En Línea]. Disponible en: https://www.digitalocean.com/community/tutorials/how-to-add-swap-space-on-ubuntu-16-04

[16] Dimitris A. Gritzalis, "Principles and requirements for a secure e-voting system", 2002.

[17] ONPE – Oficina Nacional de procesos electorales, "Posibilidades y límites del voto electrónico.". [En Línea]. Disponible en: https://www.web.onpe.gob.pe/modEducacion/Publicaciones/L-0026.pdf#page=77

[18] Escuela de fiscales Argentina. "Principios y garantías para un sistema de voto electrónico transparente y confiable". [En Línea]. Disponible en: https://www.slideshare.net/EscuelaDeFiscales/principios-y-garantias-para-un-sistema-de-voto-electronico-transparente-y-confiable

[19] Dimitris A. Gritzalis, Sokratis Katsikas, Lilian Mitrou. "Revisiting legal and regulatory requirements for secure e-voting", 2002.

[20] Gurusblog, "La historia de Bitcoin". [En Línea]. Disponible en: https://www.gurusblog.com/archives/historia-bitcoin/14/12/2013/

[21] Scott Driscoll, "How Bitcoin works". [En Línea]. Disponible en: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

[22] Israa Alqssem, Davor Svetinovic, "Towards Reference Architecture for Cryptocurrencies: Bitcoin Architectural Analysis".

[23] Ibad Siddiqui, "What Is Blockchain And How Does It Works? (Simplified)". [En Línea]. Disponible en: https://medium.com/coinmonks/what-the-hell-is-blockchain-and-how-does-it-works-simplified-b9372ecc26ef

[24] CCM, "Linux - 'Shell'". [En Línea]. Disponible en: https://es.ccm.net/contents/316-linux-shell

[25] UNLP - Facultad de informática. "E-Government: El voto electrónico sobre internet". [En Línea]. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/21971/Documento_completo.pdf?seque

[26] Javier Pastor. "Voto electrónico: estas son las claves para el fracaso frente a las papeletas de toda la vida.". [En Línea]. Disponible en: https://www.xataka.com/especiales/voto-electronico-estas-son-las-claves-de-su-fracasofrente-a-la-papeleta-de-toda-la-vida

[27] La vanguardia. "Por qué sólo siete países en todo el mundo han implantado el voto electrónico". [En Línea]. Disponible en: http://www.lavanguardia.com/politica/elecciones/20151218/30898019330/votoelectronico-20d-elecciones.html

[28] ProCon. "Do Electronic Voting Machines Improve the Voting Process?". [En Línea]. Disponible en: http://votingmachines.procon.org/view.resource.php?resourceID=000265