UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Modelado de un sistema de votación electrónico basado en la tecnología blockchain a través de JFrame de Java Swing

AUTORA:

Lindao Rodriguez, Irene Manuela

Trabajo de Titulación previo a la obtención del título de

INGENIERA EN TELECOMUNICACIONES

TUTOR:

Ing. Suárez Murillo, Efraín Oswaldo

Guayaquil, Ecuador

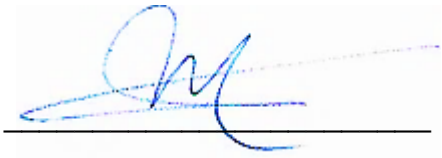
7 de marzo del 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Srta. **Lindao Rodriguez, Irene Manuela** como requerimiento para la obtención del título de **INGENIERA EN TELECOMUNICACIONES**.

TUTOR



Ing. Suárez Murillo, Efraín Oswaldo

DIRECTOR DE CARRERA

M. Sc. Heras Sánchez, Miguel Armando

Guayaquil, a los 7 días del mes de marzo del año 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Lindao Rodriguez, Irene Manuela**

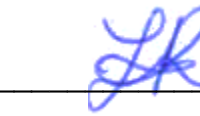
DECLARO QUE:

El trabajo de titulación **"Modelado de un sistema de votación electrónico basado en la seguridad de la tecnología blockchain a través de JFrame de Java Swing"** previo a la obtención del Título de **Ingeniera en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 7 días del mes de marzo del año 2022

EL AUTOR



Lindao Rodriguez, Irene Manuela

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

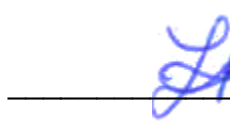
AUTORIZACIÓN

Yo, **Lindao Rodriguez, Irene Manuela**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **"Modelado de un sistema de votación electrónico basado en la tecnología blockchain a través de JFrame de Java Swing"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

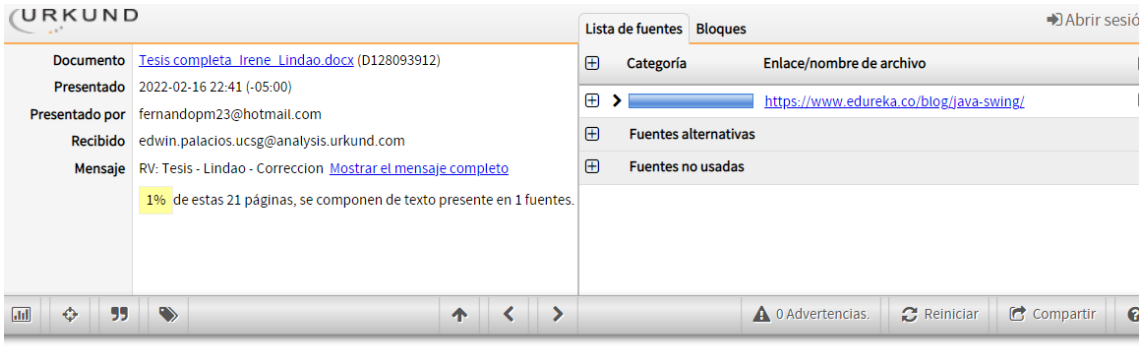
Guayaquil, a los 7 días del mes de marzo del año 2022

EL AUTOR



Lindao Rodriguez, Irene Manuela

REPORTE DE URKUND



UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA: Modelado de un sistema de votación electrónico basado en la tecnología blockchain a través de JFrame de Java Swing

AUTORA: Lindao Rodriguez, Irene Manuela

Trabajo de Titulación previo a la obtención del título de INGENIERA EN TELECOMUNICACIONES

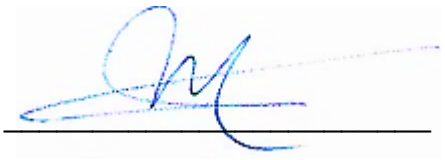
TUTOR: Ing. Suárez Murillo, Efraín Oswaldo

Guayaquil, Ecuador 20 de Febrero del 2022

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

TUTOR



Ing. Suárez Murillo, Efraín Oswaldo

DEDICATORIA

Este trabajo va dedicado a mi mamá y a mi papá, quienes han sido un apoyo moral y económico en estos años de estudio; a mis abuelos consentidores e inspiradores, que sin ellos tampoco lo hubiese logrado, muchas gracias a todos ustedes, esto es por y para ustedes.

EL AUTOR

Lindao Rodriguez, Irene Manuela

AGRADECIMIENTO

Estoy profundamente agradecida con mis padres quienes han sido un gran ejemplo, inspiración y pilar fundamental en mi vida, así como con mis abuelos, que a pesar de que algunos ya no estén físicamente conmigo, les agradezco por sus palabras de aliento. También, a la Universidad Católica de Santiago de Guayaquil por brindarme educación no solo sobre mi carrera sino también sobre valores humanos; y también a las personas que me han apoyado en este camino.

Gracias a mi tutor el Ing. Efrain Suarez, quien, con su paciencia, guía y consejos, estuvo ayudándome en este trabajo de titulación.

EL AUTOR

Lindao Rodriguez, Irene Manuela

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. ROMERO PAZ, MANUEL DE JESUS

DECANO

f. _____

M. Sc. PALACIOS MELÉNDEZ, EDWIN FERNANDO

COORDINADOR DEL ÁREA

f. _____

M. Sc. PHILCO ASQUI, LUIS ORLANDO

OPONENTE

ÍNDICE

ÍNDICE DE FIGURAS

Capítulo 2

Capítulo 3

ÍNDICE DE TABLAS

RESUMEN

Para el desarrollo del presente trabajo de titulación, se optó por usar Java swing en conjunto con JFrame en el software NetBeans, para modelar un sistema de votación apoyado en la nueva tecnología llamada Blockchain la cual ofrece seguridad al ciudadano de que su decisión no se podrá alterar ni modificar; anonimato para los votantes; y base de datos en donde estarán registrados quienes pueden ejercer su derecho al voto; estas cualidades son fundamentales para el desarrollo de este tipo de sistemas, por ello, se realizó un modelo de un sistema de votación, en dónde los ciudadanos ecuatorianos pueden acceder al voto desde la comodidad de su hogar, pero primero deben identificarse escribiendo sus datos personales, después de escribirlos correctamente, se podrá acceder a la ventana dónde aparecerá los diferentes partidos o movimientos políticos y candidatos aprobados por la CNE, y de esa manera podrá hacer su ejercicio al voto. Así, se podrá evitar aglomeraciones y contratiempos que surgen al momento de votar, cuando las personas se trasladan a su recinto electoral.

Palabras claves: Blockchain, Seguridad, Java, Votación, Modelado

ABSTRACT

For the development of this work degree, Java Swing going to be use in conjunction with JFrame in NetBeans software, to model a voting system supported by the new technology called Blockchain which provides security to citizens and they know that their decision cannot be altered or modified; also, has anonymity for voters; and database where people are registered; These qualities are fundamental for the development of this type of systems, for that reason, a model of a voting system was made, and Ecuadorian citizens can access the vote from the comfort of their home, but first, they must identify themselves by writing their personal data, after writing them correctly, they can access to another window that shows the lists and candidates approved by the CNE, and in this way they can vote. Thus, it will be possible to avoid crowds and inconveniences that arise at the time of voting when people move to their electoral precinct.

Keywords: Blockchain, Security, Java, Voting, Modelling

Capítulo 1: Descripción General del Trabajo de Titulación

1.1 Introducción

Ecuador es un país democrático en donde sus ciudadanos tienen la posibilidad y el deber de participar en las decisiones del Estado mediante el voto de las distintas dignidades. En el primer semestre del año 2021, se hizo el ejercicio del voto, pero por la emergencia sanitaria que se vive en el mundo por la COVID-19, realizar este acto patriótico tuvo algunos inconvenientes, hubo largas filas y mucha gente enferma no pudo acudir a sus recintos electorales. Por ello, surgió la idea de solucionar los problemas que se puedan presentar, a través de la tecnología, proponiendo la formación de un modelo de sistema de votación basado en el conjunto de técnicas blockchain, el cual no está muy profundizado debido a que es un concepto que se ha ido desarrollando en la última década, por esa razón, para visualizar como se vería dicho sistema, se utilizará la herramienta que ofrece Java Swing, llamada JFrame, y de esa manera reflejar que aspectos debería tener la plataforma de votaciones en blockchain.

Se eligió la tecnología blockchain para el desarrollo del sistema de votación debido a que este hace el uso de la seguridad criptográfica en las transacciones, las cuales dan la posibilidad de establecer contratos inteligentes.

1.2 Antecedentes

Ecuador es un país democrático que tiene un sistema de voto tradicional, en donde sus ciudadanos deben acercarse durante las horas de atención del día asignado a sus respectivos recintos y juntas para ejercer su deber al voto.

Si bien hay tecnologías de información que presentan varias opciones como E-Voting y Remote E-Voting, las cuales sirven para gestionar los procesos electorales, estas son muy distantes de blockchain y la seguridad que este puede ofrecer durante el ejercicio del voto.

En las últimas décadas la tecnología ha crecido de manera progresiva, tanto así que en la actualidad se puede hacer transacciones a través de

criptomonedas; a raíz de estos cambios muchos creen que la cadena de bloques (blockchain) nació a partir de la introducción de la moneda “Bitcoin”, puesto que esta información la afirma el japonés Satoshi Nakamoto en su trabajo de investigación, pero, en realidad, ya había un estudio sobre el blockchain o mejor dicho la estructura de la marca o sellado de tiempo, el cual fue realizado 20 años antes del nacimiento del Bitcoin.

Scott Stornetta y su compañero de trabajo Stuart Haber se conocieron en Bell Labs, Stornetta convenció a Haber de que la inmutabilidad de los registros digitales era un problema en el que merecía la pena trabajar. Su solución inicial se basaba en funciones hash (ampliamente utilizado en criptografía, es un resultado de longitud fija de pocos bytes obtenido criptográficamente a partir de documentos de diferente longitud y certificados digitales). Esto vincula el hash irremediablemente al documento. De esta manera surgió el Servicio de Sellado de Tiempo (TSS), en donde el cliente lo emplearía para que el TSS estampe entonces el sello de tiempo del documento y lo certifique.

También, se encuentra otra ampliación en el documento, llamada “linking". La cual trata sobre una cadena que enlaza los documentos entre sí, y el certificado de cada documento contendría un enlace con el documento anterior de la secuencia.

1.3 Definición del problema

En tiempos de pandemia como la que el mundo está atravesando en estos momentos, hay que evitar salir y aglomerarse, como ejemplo de que ello, está las elecciones electorales del año 2021, en las cuales los ciudadanos ecuatorianos pasaron muchas horas esperando para ejercer su derecho al voto, y muchos otros no pudieron acudir a los recintos electorales asignados, ya sea porque cambiaron de residencia o por enfermedad.

1.4 Justificación del problema

Considerando lo planteado en el punto anterior, resulta apropiado ofrecer una forma alternativa a la convencional de ejercer el voto, con la

seguridad de que este no sea alterado. Mediante un modelado de un sistema de votación basado en la tecnología blockchain a través de Java JFrame, que simule como seria el sistema de votación, para garantizar el libre ejercicio a los ciudadanos ecuatorianos.

1.5 Objetivos

1.5.1 Objetivo general

Modelar un sistema de votación apoyado en la seguridad que ofrece blockchain, a través la herramienta JFrame proporcionada por Java Swing, para que los ciudadanos ecuatorianos puedan ejercer el voto desde sus hogares.

1.5.2 Objetivos específicos

- Describir las características de la cadena de bloques o blockchain.
- Diseñar diagramas de flujo en correlación al registro de votos en la blockchain.
- Relacionar el modelado de Java Swing con la tecnología Blockchain

1.6 Metodología de la investigación

En el presente trabajo para la obtención de título de tercer nivel, se realizará un análisis documental de varias fuentes para recopilar información sobre la nueva tecnología blockchain y sus propiedades. Además, se realizará un modelado de como esta tecnología se visualizaría para sistemas de votación.

Capítulo 2: Fundamentación teórica

2.1 Historia e introducción a la tecnología Blockchain

El primer diseño documentado de blockchain fue en 2008, y la primera implementación de código abierto de blockchain se desplegó en 2009 como un elemento integral de Bitcoin, el primer sistema de moneda digital descentralizada para distribuir bitcoins a través del lanzamiento de código abierto del software peer-to-peer de Bitcoin. Ambos fueron propuestos por una entidad anónima, conocida como Satoshi Nakamoto (Zhang et al., 2019).

Según Luque, 2020, el concepto de "blockchain" se hizo popular con la publicación del libro blanco "Bitcoin: A Peer to Peer Electronic Cash System", de Satoshi Nakamoto, pero, este artículo es en realidad una colección del conjunto de ideas publicadas que otros autores sacaron a la luz en el pasado, los escritores que inventaron el concepto de la cadena de bloques son Scott Stornetta y su compañero de trabajo Stuart Haber.

A finales de los años 80's Stornetta convenció a Haber de que la intangibilidad de los registros digitales era un problema en el que merecía la pena trabajar. Su solución inicial se basaba en funciones hash y certificados digitales. Para entenderlo se puede decir que un hash es un concepto bien conocido y ampliamente utilizado en criptografía. También, se lo llama "un resumen de mensajes" y es un resultado de longitud fija (normalmente de unos pocos bytes), obtenido criptográficamente a partir de documentos de diversa longitud. El hash cambia, incluso cuando cambia un bit del documento original. Esto vincula lo vincula de forma irrevocable al documento. En la figura 2.1 se muestra el esquema de TSS basado en el documento de Nakamoto acerca del bitcoin- (Bharathan, 2020).

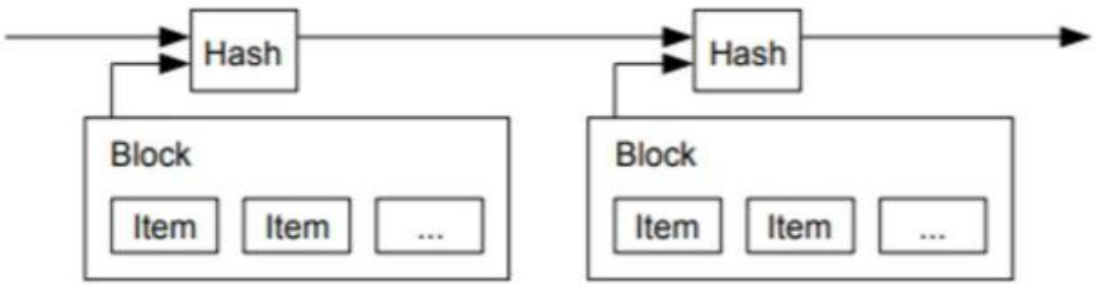


Figura 2. 1: TSS del documento de Bitcoin de Nakamoto
Fuente: (Bharathan, 2020)

Debido al documento en el que trabajaron juntos Stornetta y Haber, se desarrolló el concepto de “Servicio de Sellado de Tiempo” o Time Stamping Service (TSS). El TSS sellaría el documento hash y lo certificaría. Otra extensión de esta investigación es la sección titulada "linking", que presenta una cadena de documentos para introducir una secuencia temporal. Se trataría de una cadena que enlaza los documentos entre sí, y el certificado de cada documento contendría un enlace con el documento anterior de la secuencia (Bharathan, 2020).

Así nació la primera solución al problema de crear una marca de tiempo vinculada, inmutable e irrefutable, de una serie de documentos digitales, que puede llamarse blockchain, lo que ya existía en el trabajo de Stornetta y Haber, hace unos veinte años antes de Bitcoin (Bharathan, 2020).

La base de blockchain es la Tecnología de Libro Mayor Distribuido o Distributed ledger technology (DLT). La DLT ofrece un mecanismo de validación por consenso a través de una red de ordenadores que facilita las transacciones entre pares sin necesidad de un intermediario o una autoridad centralizada que actualice y mantenga la información generada por las transacciones. Cada transacción se valida y, junto con un grupo de transacciones validadas, se añade como un nuevo "bloque" a una cadena de transacciones ya existente, dando lugar al nombre de "blockchain". Una vez que una transacción se ha añadido a la cadena, generalmente no puede ser alterada o eliminada (Rennock et al., 2018).

Blockchain ofrece una forma innovadora de almacenar información, ejecutar transacciones, y desempeñar funciones. Para muchos, la cadena de bloques es un avance tecnológico en el campo de la criptografía y la ciberseguridad, con ejemplos de uso que van desde los sistemas de criptomoneda implantados a nivel mundial como Bitcoin, a los contratos inteligentes, las redes inteligentes en el Internet de las cosas, etc (Zhang et al., 2019).

El sistema Bitcoin utiliza la blockchain como su libro de contabilidad público distribuido, el cual registra y verifica todas las transacciones de bitcoin en el sistema abierto de red peer-to-peer de Bitcoin. Una innovación notable de blockchain acerca de las criptomonedas, es su capacidad para evitar el doble gasto en las transacciones de bitcoin en una red peer-to-peer (red de

pares, red entre iguales o red entre pares) totalmente descentralizada, sin depender de ninguna autoridad central de confianza. de confianza (Zhang et al., 2019).

Como registro seguro, blockchain organiza la creciente lista de registros de transacciones en una cadena de bloques que se expande jerárquicamente y en donde cada bloque está protegido por técnicas de criptografía para reforzar la integridad de sus registros de transacciones. Los nuevos bloques sólo pueden incorporarse a la cadena de bloques global tras superar el procedimiento de consenso descentralizado(Zhang et al., 2019).

2.2 Tipos de Blockchain

Hay tres tipos de redes blockchain:

- Blockchain con permiso: Estas redes son redes propias que utilizan individuos o entidades específicas para realizar transacciones, como ejemplo se plantea un grupo de bancos que procesan transacciones financieras. (Rennock et al., 2018)
- Blockchain públicas o sin permiso. Son redes de código abierto a las que cualquiera puede acceder y utilizar, como los usuarios de bitcoin que realizan transacciones entre sí utilizando bitcoin como medio de pago (Rennock et al., 2018)

A diferencia de la blockchain de bitcoin y otras redes públicas, las redes de blockchain con permiso suelen ser desarrolladas por empresas para su propio uso comercial privado. Las entidades pueden desarrollar su propia red o modificar una red básica desarrollada previamente por un proveedor. En ocasiones, un grupo de empresas de un sector puede colaborar para elaborar y compartir una red propia que facilite las transacciones entre ellas, como el consorcio R3 blockchain, que ofrece un sistema blockchain para instituciones financieras (Rennock et al., 2018).

- Blockchain de consorcio o federadas: Estas se encargan de la toma de decisiones. Están muy poco permitidas y están representadas por un grupo de empresas o individuos. Esto conduce a transacciones más rápidas y ofrece múltiples puntos de fallo, preservando así los datos. Los miembros son los encargados de realizar las

transacciones/decisiones. Pueden leer, escribir, auditar y minar datos. Ejemplos comunes de blockchain de consorcio son R3 y EWF (Energy Web Foundation) (Le et al., 2019).

2.3 Peculiaridades de blockchain

2.3.1 Características de la tecnología blockchain

Blockchain sirve para varios propósitos, y estos están basados en las siguientes características:

- Descentralización: La tecnología blockchain no depende de un sistema de transacciones centralizado para validar las transacciones. La participación de organismos centrales de confianza conlleva problemas de costes y rendimiento. Dado que no se necesita un tercero para las blockchain, éstas dependen de la criptografía y los algoritmos para mantener la consistencia de los datos en las redes distribuidas (Le et al., 2019).
- Persistencia: La validación de las transacciones es rápida en la tecnología blockchain. Las transacciones no válidas pueden ser eliminadas. Las transacciones que ya forman parte de la blockchain no pueden borrarse ni revertirse. La manipulación de los datos puede realizarse fácilmente (Le et al., 2019).
- Verificabilidad pública: La corrección del estado del sistema puede ser confirmada por cualquier usuario. Este no es el caso de los sistemas que dependen de agencias de confianza centrales. Los usuarios tienen que comunicarse con las agencias para obtener información sobre el estado correcto (Le et al., 2019).
- Transparencia: Los datos de la blockchain se actualizan para su verificación pública. Sin embargo, la cantidad de información puede estar restringida a los usuarios en función de sus privilegios (Le et al., 2019).
- Privacidad: Aunque la privacidad es más fácil de conseguir en los sistemas centralizados, las blockchain con protocolos específicos pueden permitir un cierto nivel de privacidad para salvaguardar la información sensible (Le et al., 2019).

- Integridad: La tecnología blockchain protege contra las modificaciones no autorizadas, lo que conduce a la integridad de los datos. Dado que el sistema permite la verificabilidad pública, la integridad de los datos puede ser verificada por cualquiera (Le et al., 2019).
- Redundancia: La tecnología blockchain se basa en una arquitectura descentralizada. Esto significa que los datos se duplican en todos los escritores, a diferencia de los sistemas centralizados que dependen de copias de seguridad y servidores físicos para lograr la redundancia de los datos(Le et al., 2019).
- Ancla de confianza: El ancla de confianza es la entidad responsable de proporcionar acceso de lectura y escritura a un sistema. Son las máximas autoridades y poseen derechos de concesión y revocación (Le et al., 2019).

2.3.2 Características básicas de blockchain al realizar transacciones

La tecnología blockchain comparte ciertas características al momento de realizar una transacción, las cuales son:

- Registros en tiempo real: Los libros de contabilidad distribuidos se actualizan en tiempo real a medida que se producen las transacciones y otros eventos, con un software que automatiza el proceso. Estas características garantizan que cada participante de la red tenga su propio registro actualizado de las transacciones, lo que reduce las oportunidades de fraude. El proceso automatizado y la ausencia de un registro centralizado también aumentan la eficiencia y generan un ahorro de costes (Rennock et al., 2018).
- Registros inmutables: La tecnología blockchain permite a las entidades crear registros de transacciones permanentes e inmutables. Esta capacidad ofrece un beneficio comercial, pero también puede aumentar el riesgo regulatorio para algunas partes. Los reguladores pueden obtener permiso para acceder a los historiales completos de las transacciones en caso de una investigación que implique transacciones registradas en una blockchain, lo que hace más difícil que las partes

argumenten que carecen de registros adecuados de las transacciones. Además, mantener un registro permanente de ciertas transacciones y usuarios a través de una blockchain puede implicar regulaciones de privacidad de datos, particularmente porque los reguladores se centran cada vez más en la protección de la privacidad del consumidor (Rennock et al., 2018)

- Anonimato: La tecnología blockchain facilita que los usuarios de la red sean seudónimos, lo que tiene ramificaciones para los operadores de redes sujetos a las regulaciones contra el lavado de dinero (AML - Anti-Money Laundering) y de conocimiento del cliente (KYC)(Rennock et al., 2018).
- Riesgo de ciberseguridad: Las redes de blockchain son los objetivos favoritos de los hackers. Aunque ninguna blockchain ha sido hackeada o manipulada con éxito, las empresas y la tecnología que la rodean sí lo han sido. Los incidentes de seguridad han ido desde interrupciones mundanas del servicio hasta robos más graves de datos sensibles y criptomonedas valiosas, aunque la estructura descentralizada de las redes blockchain las hace más resistentes a los ataques o manipulaciones en toda la red (Rennock et al., 2018).
- Implicaciones fiscales: Las transacciones de blockchain en las que interviene una moneda virtual pueden dar lugar a consecuencias fiscales imprevistas en función del tratamiento que la autoridad fiscal aplicable dé a la moneda virtual. El Servicio de Impuestos Internos (IRS) de EE.UU., por ejemplo, trata la moneda virtual como una propiedad, lo que significa que una transacción puede crear la necesidad de reconocer una ganancia o pérdida en la criptodivisa intercambiada (Rennock et al., 2018).

En la figura 2.2 se puede observar una representación visual de blockchain, en donde se quiere transferir el dinero,

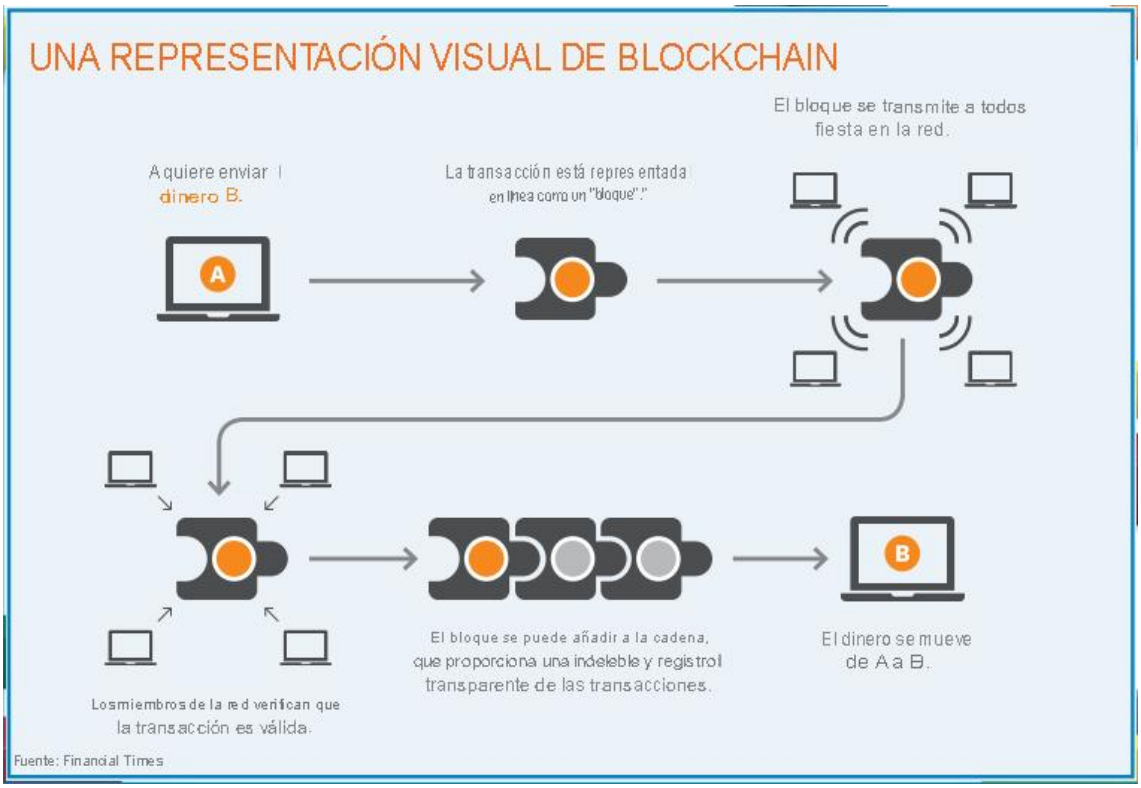


Figura 2. 2: Representación visual de Blockchain
Fuente: (Rennock et al., 2018)

2.4 Arquitectura de Blockchain

Blockchain utiliza bloques y algoritmos firmados digitalmente para realizar transacciones y documentaciones rápidas y en tiempo real. También, incorporan bloques que se basan en punteros los cuales conectan datos de bloques anteriores. Estos bloques no pueden ser alterados fácilmente, lo que garantiza la seguridad. Las validaciones de nuevos bloques también se basan en algoritmos de consenso (Le et al., 2019).

Según (Saghiri, 2019), la mayoría de las aplicaciones basadas en blockchain se obtienen a partir de tres elementos que se describen a continuación:

- Un sistema que maneja el sistema blockchain.
- Un sistema que utiliza la tecnología blockchain para gestionar los requisitos definidos por el usuario para la aplicación.
- Una interfaz de programación de aplicaciones (API) que se utiliza para gestionar nuevos requisitos teniendo en cuenta los objetivos de la aplicación.

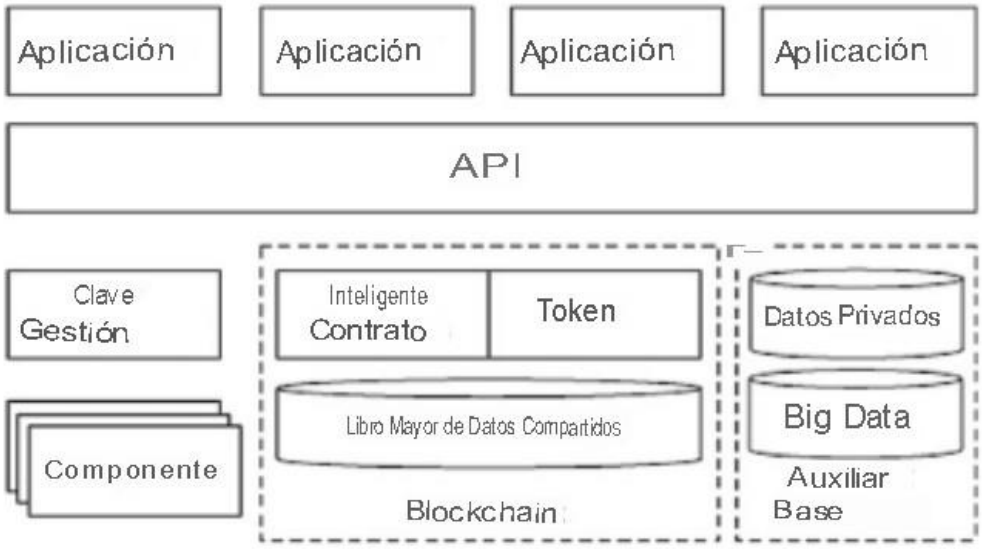


Figura 2. 3: Elementos de un sistema basado en blockchain
Fuente: (Saghiri, 2019)

Según (Le et al., 2019), blockchain utiliza bloques y algoritmos firmados digitalmente para realizar transacciones y documentaciones de forma rápida y en tiempo real, que además se cifran. Se incorporan bloques que se basan en punteros que conectan datos de bloques anteriores, los cuales no pueden ser alterados fácilmente, lo que garantiza la seguridad. Las validaciones de nuevos bloques también se cimentan en algoritmos de consenso. La transacción de extremo a extremo de la cadena de bloques sigue un mecanismo determinado. Su arquitectura se fundamenta en los siguientes componentes:

1. Plataforma blockchain: El blockchain puede definirse como una aplicación que se ejecuta en una red distribuida. Es un sistema de transacciones descentralizado que es transparente en el sentido de que cualquier nodo que maneje un software de blockchain es capaz de manejarla toda. Los datos correspondientes se almacenan en un archivo plano o en una base de datos relacional. La aplicación instalada se sincroniza del servidor a los nodos. Los servidores engloban registros de transacciones basados en protocolos criptográficos y algoritmos de consenso. Dado que el software es robusto, es prácticamente imposible irrumpir en las aplicaciones que se ejecutan. Las transacciones no necesitan de terceros para su autentificación y validación, estas son verificadas por los nodos de una red peer-to-peer. Cuando muchos nodos están de acuerdo con respecto

a sus bloques en las bases de datos individuales, se dice que están en consenso. La cadena de bloques tiene tres capas principales. También, los clientes soportados son full, web y mobile. La capa de blockchain se encarga de mantener la cadena de bloques, mientras que las capas de protocolo y de cliente proporcionan el protocolo peer-to-peer y las reglas de consenso. En la figura 2.4 se muestra el diagrama de la arquitectura de blockchain, en donde se muestran las capas principales de este (Le et al., 2019)

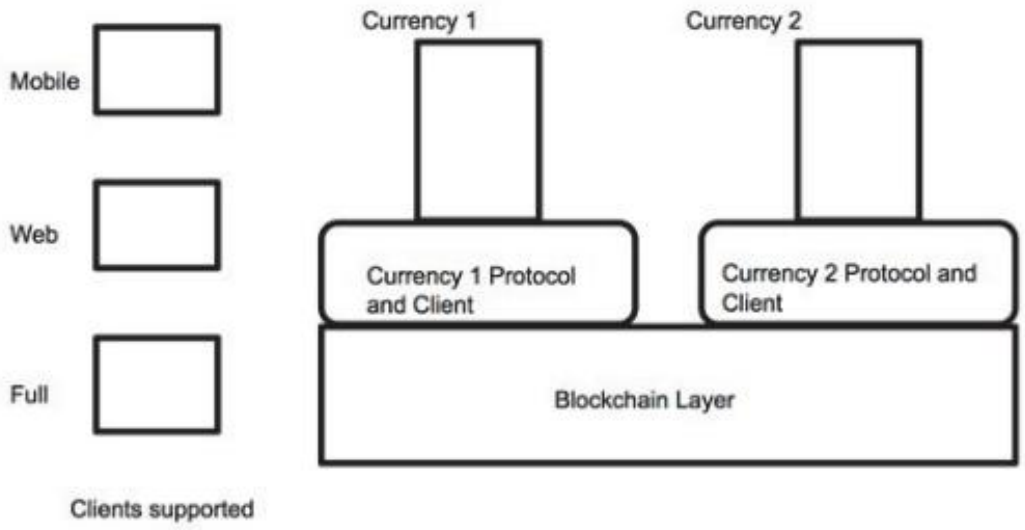


Figura 2. 4: Diagrama de la arquitectura de Blockchain
Fuente: (Le et al., 2019)

2. Nodos de blockchain: La tecnología blockchain opera en la red colaboradora peer-to-peer (P2P) y en el protocolo de Internet. Esta red tiene nodos responsables de mantener copias duplicadas de la base de datos que contienen información relacionada con el pago y la propiedad. Las transacciones hacen que los nodos se pongan de acuerdo en las actualizaciones. Los nodos que almacenan una parte de la base de datos verifican las transacciones utilizando la verificación de pago simple (SPV). En el punto 2.5 del presente trabajo se explayará con más detalle acerca de esta red (Le et al., 2019).

3. Pila de protocolos de red: Los nodos de la blockchain pueden descubrir y contactar con otros nodos válidos. El intercambio de mensajes de blockchain sigue el proceso de handshaking entre nodos para intercambiar información a través de la red. Esta capa también puede utilizarse para dar soporte a otras aplicaciones. En la figura 2.5 se muestra el flujo de información y arquitectura de la tecnología de cadena de bloques, en donde se puede observar la transferencia de información de los servidores (Le et al., 2019).

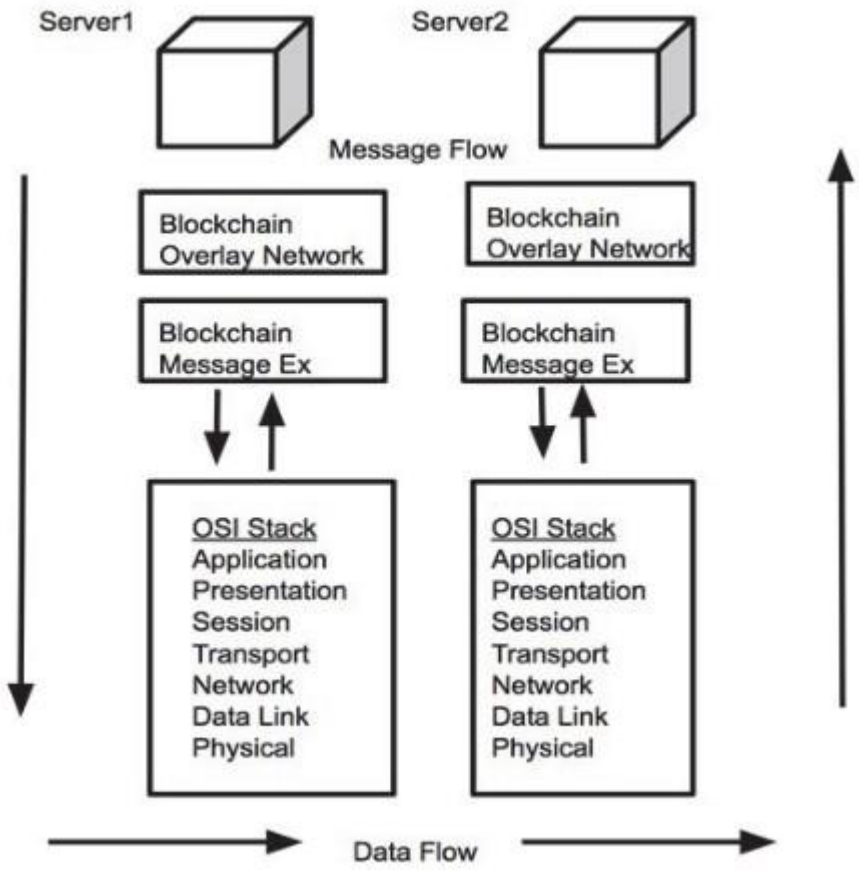


Figura 2. 5: Flujo de información y arquitectura de la tecnología blockchain
Fuente: (Le et al., 2019)

4. Transacciones: Las blockchain son utilizadas por las aplicaciones para marcar el tiempo de las transacciones. Los registros en una blockchain existen como transacciones y bloques. Las transacciones pueden ser creadas por los clientes o las aplicaciones de los clientes. Tienen datos significativos que contribuyen al blockchain. Las secuencias de transacciones se almacenan en bloques y estos bloques son creados por nodos mineros. Cuando se registra una transacción en un sistema, se añade a la red de nodos de blockchain una transacción recién generada. Los nodos menores

comprueban su validez, tras lo cual se somete a una técnica de hashing criptográfico para generar una secuencia única de caracteres. Se colabora con otras transacciones y el hash recién generado se almacena con otros metadatos en una cabecera de estructura de datos. Así se crea un bloque para el que la cabecera sirve de clave. Esto puede conducir a la creación del bloque hijo siguiente (Le et al., 2019).

2.5 Redes Peer-to-peer (P2P, red de pares, red entre iguales o red entre pares)

La red peer-to-peer nació gracias al aumento de la capacidad de procesamiento de los ordenadores, en conjunto con la disminución de su precio.(Saghiri, 2019)

La arquitectura de Blockchain está basada en las redes peer-to-peer, las cuales son sistemas distribuidos, es decir que, son una serie de ordenadores conectados a nodos. Esta red se basa en el intercambio de información entre pares, sin depender de un sistema en concreto. En este tipo de conexiones, todos los pares se consideran iguales (es decir hacen la función de cliente y servidor) y se conectan entre sí con el fin de compartir dispositivos, información o datos. En la figura 2.6 se muestra un diagrama, en donde las transacciones se convierten en bloques. (Saghiri, 2019) .

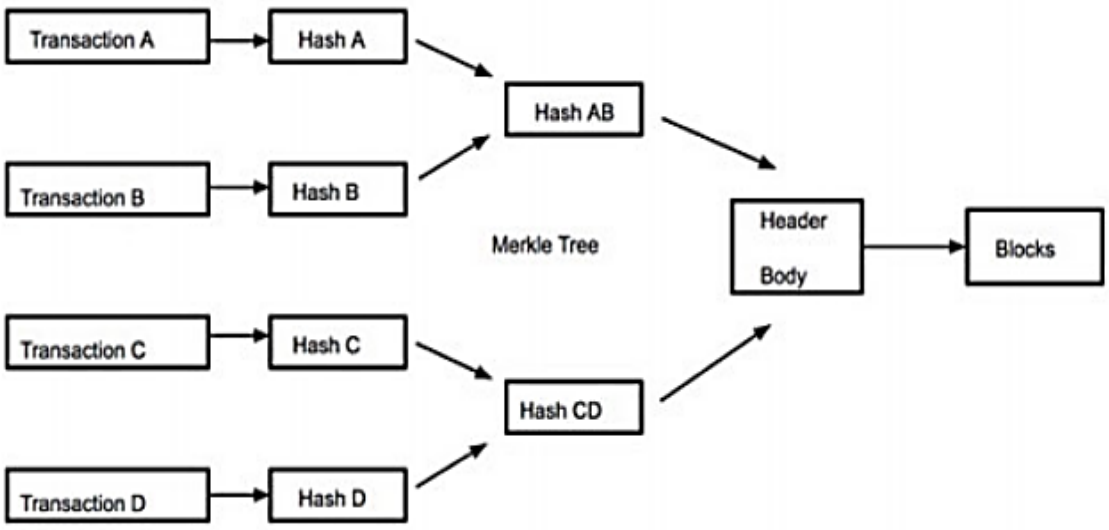


Figura 2. 6: Cuando una transacción se convierte en bloques
Fuente: (Le et al., 2019)

En la figura 2.7 se puede observar una conexión p2p. Según (Saghiri, 2019), las redes entre pares tienen características únicas que permiten que puedan ser clasificadas. Algunas de estas características son:

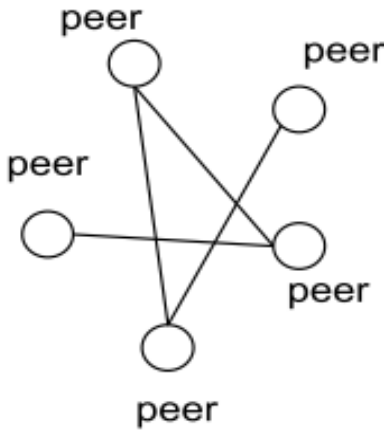


Figura 2. 7: Conexión de una red peer-to-peer
Fuente: (Saghiri, 2019)

- El rol simétrico: Cada par desempeña el rol de cliente, así como el de servidor. En otras palabras, las partes asociadas de un software peer-to-peer, al instalarse serán capaces de funcionar para los dos roles.
- Adaptabilidad: La escala de las redes P2P es la más completa, incluye el uso de toda la potencia de procesamiento disponible. Los sistemas distribuidos tradicionales no hacen hincapié en este nivel de escalabilidad.
- Heterogeneidad: Las redes P2P, desde el punto de vista de las capacidades de hardware, representan de alguna manera el concepto de heterogeneidad. No se hace hincapié en los pares en términos de recursos de almacenamiento o procesamiento.
- Control distribuido: En el caso más ideal, no existe un control centralizado para gestionar estos sistemas. Esta es una característica destacada de este tipo de sistemas.
- Dinamismo: Las redes peer-to-peer suelen funcionar en entornos dinámicos. La topología puede cambiar rápidamente debido a la inestabilidad de las conexiones entre pares.

2.5.1 Clasificación de las redes peer-to-peer

Según (Saghiri, 2019) el P2P se clasifica en tres, pero dichas clasificaciones tiene subdivisiones las cuales son:

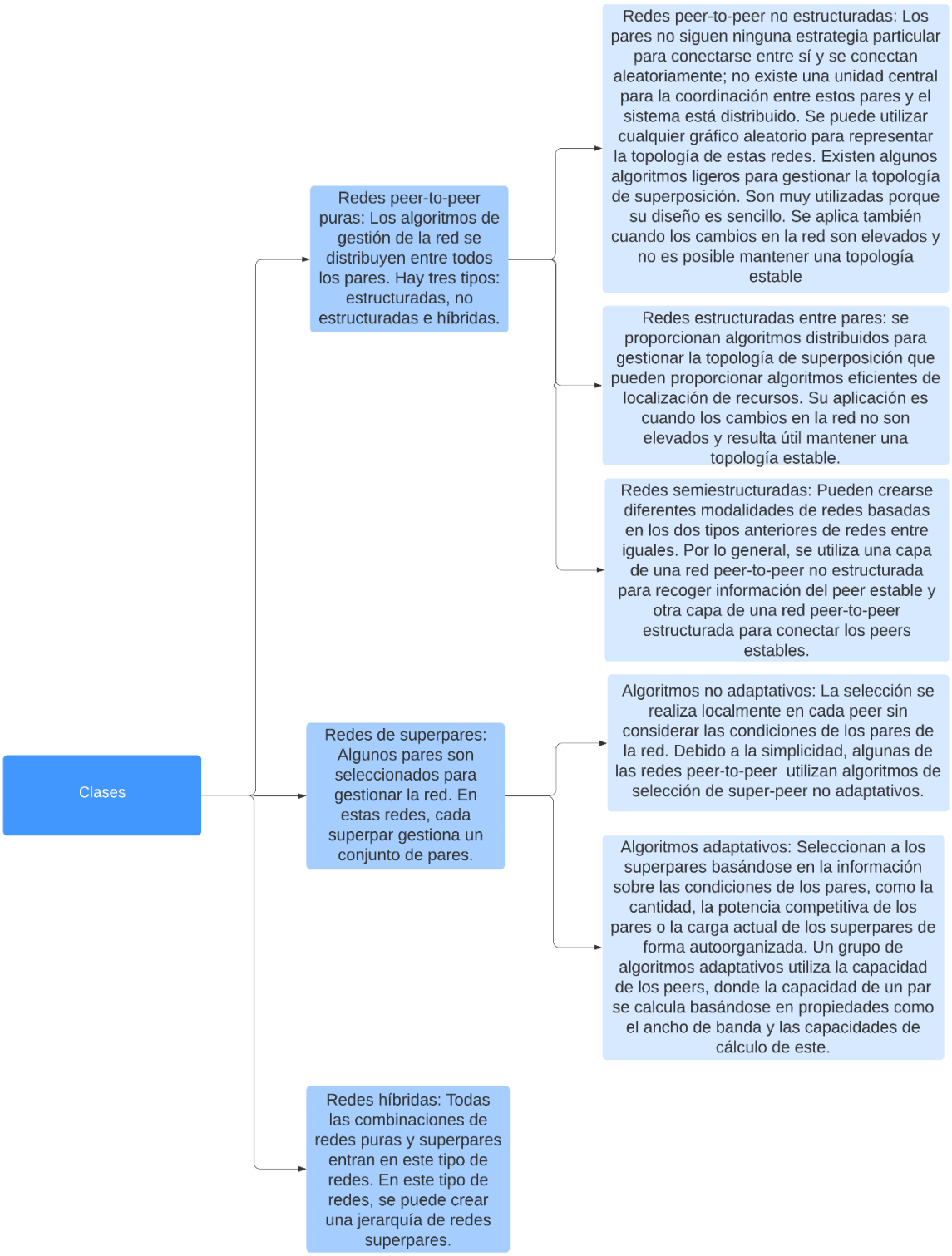


Figura 2. 8: Clasificación de las redes peer-to-peer
Fuente: Elaboración propia con información del estudio realizado por (Saghiri, 2019)

2.5.2 Mecanismos de gestión de las redes peer-to-peer

Según (Saghiri, 2019), como se ha mencionado anteriormente, una de las características importantes de las redes peer-to-peer es el dinamismo. En estos sistemas, los pares se conectan a la red sin un orden determinado. En otras palabras, las condiciones de la red cambian continuamente, y a veces no serán predecibles, y si no hay mecanismos de gestión eficaces en estas redes, las condiciones de la red llevarán rápidamente a condiciones inaceptables. Esta característica tiene un gran impacto en el diseño de algoritmos de gestión en estas redes. Teniendo en cuenta el problema mencionado, en la literatura se han descrito diferentes enfoques para el diseño de mecanismos de gestión. Algunos de ellos son:

- Enfoque de inspiración biológica
- Enfoque basado en el aprendizaje por refuerzo
- Enfoque de redes cognitivas
- Enfoque basado en la ontología y la web semántica
- Enfoque basado en la teoría de los gráficos
- Enfoque basado en la teoría de los juegos
- Enfoque heurístico y de optimización entre capas

2.5.3 Aplicaciones de las redes peer-to-peer

Según (Saghiri, 2019), en la última década, las redes peer-to-peer se utilizan como infraestructura de una amplia gama de aplicaciones. Algunas de estas aplicaciones son:

- Intercambio de archivos: Muchas aplicaciones de intercambio de archivos utilizan redes entre pares. Una ventaja de estos sistemas es que no invierten en costosos servidores (Saghiri, 2019).
- Streaming de vídeo: Recientemente, las tecnologías de streaming peer-to-peer han presentado una tecnología revolucionaria llamada (P2PTV) este servicio. En estas tecnologías, cada par puede iniciar un proceso de transmisión en vivo. Algunas de las aplicaciones más conocidas de esta categoría son Zatoo, PPlive, Tribler y LiveStation (Saghiri, 2019).

- Computación en la nube: El diseño tradicional estos sistemas ha cambiado debido a las redes peer-to-peer. La nube entre redes aporta una arquitectura adaptable para estas (Saghiri, 2019).
- Computación en red: Una red entre iguales puede utilizarse como infraestructura para compartir la potencia de cálculo. Su objetivo es proporcionar un fácil acceso a grandes cantidades de recursos computacionales para cada par (Saghiri, 2019).
- Sistema de mensajería: Debido a la naturaleza de los sistemas de mensajería peer-to-peer, que no tienen servidor, estas redes han recibido mucha atención en una amplia gama de aplicaciones (Saghiri, 2019).
- Bases de datos: Las bases de datos peer-to-peer, como OrbitDB, admiten databases distribuidas y sin servidor (Saghiri, 2019).
- Motores de búsqueda: Los motores de búsqueda peer-to-peer, como FAROO, no utilizan servidores centrales costosos (Saghiri, 2019).
- Almacenamiento: Las redes de almacenamiento peer-to-peer permiten guardar y recuperar archivos remotos entre millones de pares.
- Anonimato: Utilizando la criptografía, estas redes con peer-to-peer, permiten la comunicación entre redes con un alto grado de no tener y que sea difícil de revelar la identidad de las personas.
- Seguro médico: Los seguros peer-to-peer es una red de riesgos compartido. En este sistema, un grupo de personas unen sus “premiums” para asegurarse contra un riesgo.
- Alojamiento web: La red entre iguales se utiliza para distribuir el acceso a las páginas web en el alojamiento web entre pares.
- Sistema de dinero en línea: Bitcoin es un conocido sistema de dinero en línea que utiliza redes entre iguales. Hay muchos proyectos, como IOTA, Monero y Ethereum, similares a Bitcoin, que intentan gestionar las criptomonedas utilizando redes entre iguales.

En la figura 2.9 se puede observar las aplicaciones para las redes P2P, en donde se refleja que se puede compartir archivos; hacer streaming de videos; nube; la red de computación, sistema de mensaje; base de datos;

búsqueda; almacenamiento; anonimato; alojamiento web; y el sistema de dinero en línea extendido a bitcoin.

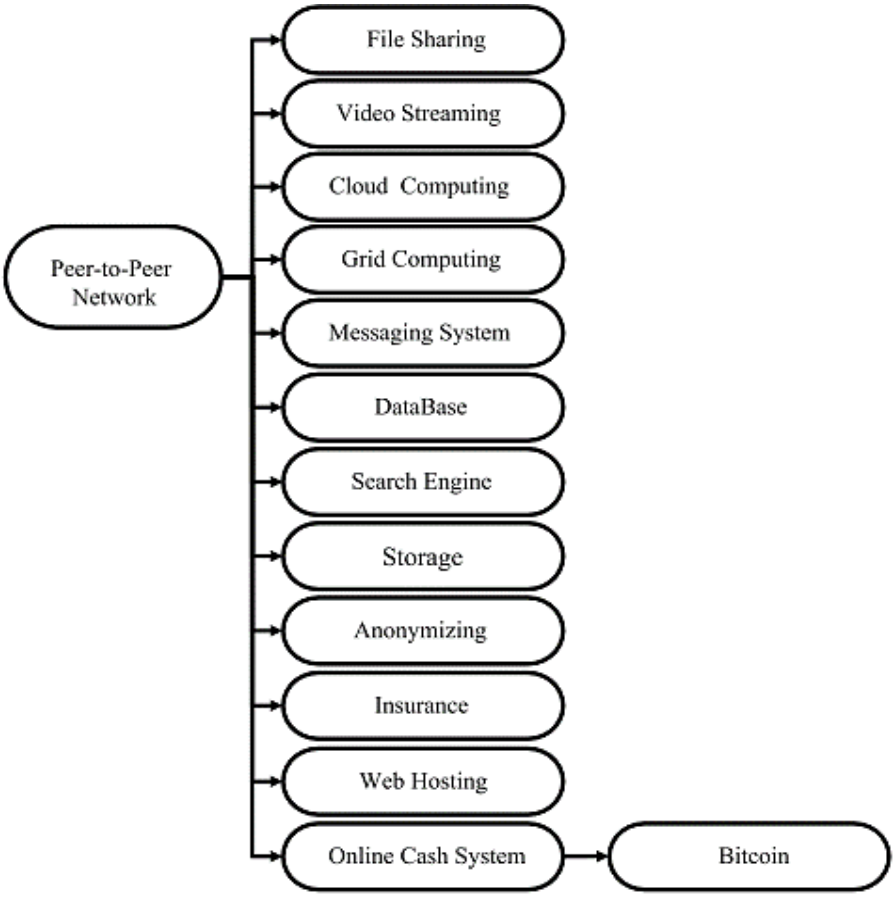


Figura 2. 9: Aplicaciones para las redes P2P
Fuente: (Saghiri,2019)

En las aplicaciones basadas en blockchain, como Bitcoin, las redes peer-to-peer se utilizan para gestionar un libro de contabilidad de forma distribuida. En estos sistemas, el libro de contabilidad puede verse como una memoria compartida con alta seguridad. Se han desarrollado muchos algoritmos distribuidos para el consenso, la gestión de bloques y la elección de líderes para los mineros en la blockchain, teniendo en cuenta las características de las redes entre pares. Cabe señalar que las tecnologías blockchain introdujeron nuevos términos como libro mayor, mineros (miners), contratos inteligentes, POW (Proof-of-Work) y POS (Proof-of-Stake) para sus redes entre iguales. Por ejemplo, en las redes P2P tradicionales, utiliza super-

peer en lugar de minero. Un nodo “miner” trata de ejecutar algunos algoritmos de gestión y sigue sus beneficios. Como otro caso, se puede utilizar un protocolo en lugar de un contrato inteligente. Un contrato inteligente es un protocolo designado para facilitar, verificar y hacer cumplir la negociación de un contrato de manera totalmente digital. Los contratos inteligentes desempeñarán un papel clave en las Organizaciones Autónomas Distribuidas (DAO) en un futuro próximo. Además de la tecnología de libro mayor distribuido, en la literatura se presentan varias tecnologías como DAG (Directed Acyclic Graph) y Hash graph para gestionar las transacciones (Saghiri, 2019).

2.6 Seguridad de blockchain

Las propiedades básicas de seguridad de blockchain provienen tanto de los avances en criptografía como del diseño e implementación de Bitcoin. Teóricamente, la primera cadena de bloques segura se formuló mediante criptografía en 1991. En 1993 se presentó una propuesta para mejorar la eficiencia de la cadena criptográfica de bloques incorporando árboles de Merkle y colocando múltiples documentos en un bloque. La cadena de bloques se construye para garantizar una serie de atributos de seguridad inherentes, como la consistencia, la resistencia a la manipulación, la resistencia a un ataque de denegación de servicio distribuido (DDoS), el seudónimo y la resistencia a un ataque de doble gasto. Sin embargo, para utilizar blockchain para el almacenamiento distribuido seguro, se requieren propiedades adicionales de seguridad y privacidad (Zhang et al., 2019).

En la Tabla 2.1 se puede observar los requerimientos, propiedades y técnicas de seguridad y privacidad de blockchain, en donde se divide entre las que son soportadas por bitcoin y las que necesitan ser mejoradas.

Tabla 2. 1:Resumen de los requerimientos, propiedades y técnicas de seguridad y privacidad de blockchain

	Requerimientos de seguridad y privacidad	Propiedades de seguridad y privacidad	Técnicas correspondientes de Seguridad y privacidad
Soportadas en Bitcoin	Consistencia	Consistencia	Algoritmos de consenso
	Integridad	Resistencia de manipulación	Almacenamiento en cadena
	Disponibilidad	Resistencia a ataques	Algoritmos de consenso con fallo
	Prevención	Resistencia a ataques dobles	Firma y verificación
	Anonimato	Pseudoanonimato	Clave pública como seudónimos
Necesita ser mejorado	Desvinculación	Desvinculación	Firma anónima
	Confidencialidad	Confidencialidad	Soluciones basadas en juegos
		Resistencia al mayor ataque	Algoritmos de consenso que no dependen de la potencia de cálculo

Fuente: Elaboración propia con información de estudio realizado por (Zhang et al., 2019)

2.7 E-voting (voto electrónico)

Es la opción de utilizar medios electrónicos para votar en referendos y elecciones. Existen diferentes sistemas, como las máquinas de votación con registro electrónico directo (DRE), que registran el voto directamente sin que éste se transmita a través de Internet u otra red: por ejemplo, la interfaz de una máquina DRE puede ser una pantalla táctil, o el votante puede rellenar la papeleta y luego escanearla en el sistema. Lo más habitual es que el voto electrónico se refiera a la votación a través de Internet mediante un ordenador personal (PC) con conexión a Internet. También hay otros medios, como los asistentes digitales personales (PDA), los teléfonos o los teléfonos móviles, que pueden utilizarse para emitir un voto electrónico (Braun, 2007).

Hay dos tipos de concepto de voto electrónico: "voto electrónico en el recinto electoral" y "voto electrónico a distancia". El "voto electrónico en el lugar de votación" se refiere a los sistemas en los que el votante emite su voto dentro de un recinto electoral o de un local similar controlado por el personal electoral, que en el caso de Ecuador es en Consejo Nacional Electoral; el "voto electrónico a distancia" se utiliza para describir aquellos sistemas en los que el votante emite su voto en cualquier lugar fuera de la junta electoral (Braun, 2007).

Hay diferentes maneras de utilizar los medios electrónicos para facilitar el voto externo. La más difícil sería permitir a los votantes que se encuentran en el extranjero transmitir un voto utilizando medios electrónicos, por ejemplo, emitiendo un voto en un PC y transmitiéndolo a la urna electrónica a través de Internet. El voto electrónico también podría llevarse a cabo en el entorno supervisado de una misión diplomática o consular (Braun, 2007).

2.8 Blockchain como servicio de votación electrónica

2.8.1 Configuración blockchain

Según (Hjalmarsson et al., 2018) para satisfacer la necesidad y los requerimientos de privacidad y seguridad en el sistema de votación electrónica se utiliza la blockchain de Prueba de Autoridad (POA). POA utiliza un algoritmo que proporciona transacciones comparativamente rápidas a través de un mecanismo de consenso basado en la identidad como participación, contando con dos nodos principales:

- Nodo de distrito: Representan cada distrito electoral. Cada nodo de distrito tiene un agente de software que interactúa de forma autónoma con el "bootnode" y gestiona el ciclo de vida del contrato inteligente en ese nodo. Cuando el administrador electoral crea una elección, se distribuye un contrato inteligente de boleta y se despliega en su nodo de distrito correspondiente. Cuando se crean los contratos inteligentes de votación, cada uno de los nodos de distrito correspondientes recibe permiso para interactuar con su contrato correspondiente. Cuando un votante individual emite su voto desde su contrato inteligente correspondiente, los datos del voto son verificados por la mayoría de

los nodos de distrito correspondientes y cada voto que acuerdan se añade a la blockchain (Hjalmarsson et al., 2018).

- Nodo de arranque (bootnode): Cada institución, con acceso autorizado a la red, alberga un bootnode, el cual es un servicio de descubrimiento y coordinación que ayuda a los nodos de distrito a descubrirse entre sí y a comunicarse. También, no mantiene ningún estado de la blockchain y se ejecuta en una IP estática para que los nodos de distrito encuentren a sus compañeros más rápidamente. Después de crear una blockchain segura y privada, el siguiente paso es definir y desplegar un contrato inteligente que represente el proceso de votación electrónica en la infraestructura de blockchain (Hjalmarsson et al., 2018).

2.8.2 Elección como contrato inteligente

La elección como contrato inteligente incluye tres partes: identificar los roles que están involucrados en el acuerdo (el acuerdo de elección en nuestro caso); el proceso de acuerdo (es decir, el proceso de elección); y las transacciones (es decir, la transacción de votación) utilizadas en el contrato inteligente (Hjalmarsson et al., 2018).

- Según (Hjalmarsson et al., 2018) los roles de elección están bajo un contrato inteligente incluyen que las partes a participar estén en un acuerdo. El proceso de elección tiene los siguientes roles:
- Administrador de la elección: Se usa para gestionar el ciclo de vida de una elección. Múltiples instituciones y empresas de confianza pueden estar inscritas en este rol. Los administradores electorales crean la elección, registran a los votantes, deciden el tiempo de vida de la elección y asignan los nodos con permiso (Hjalmarsson et al., 2018)
- Votante: Es un ciudadano con derecho a voto. Los votantes pueden autenticarse, cargar las papeletas electorales, emitir su voto y verificar su voto una vez finalizadas las elecciones (Hjalmarsson et al., 2018).

- Proceso electoral: Cada proceso electoral está representado, por un conjunto de contratos inteligentes, que son desplegados en la blockchain por los administradores electorales. Se define un contrato inteligente para cada uno de los distritos electorales. Las principales actividades del proceso electoral son las siguientes: creación de las elecciones en donde los administradores electorales crean las papeletas electorales utilizando un contrato inteligente en el que el administrador define una lista de candidatos para cada junta electoral; para el registro de los votantes deben de identificarse a través de un documento legal otorgado por el Estado ecuatoriano, para autenticar y autorizar de forma segura a los individuos elegibles. El uso de un servicio de este tipo es necesario para satisfacer el requisito de autenticación segura, ya que esto no está garantizado, por defecto,

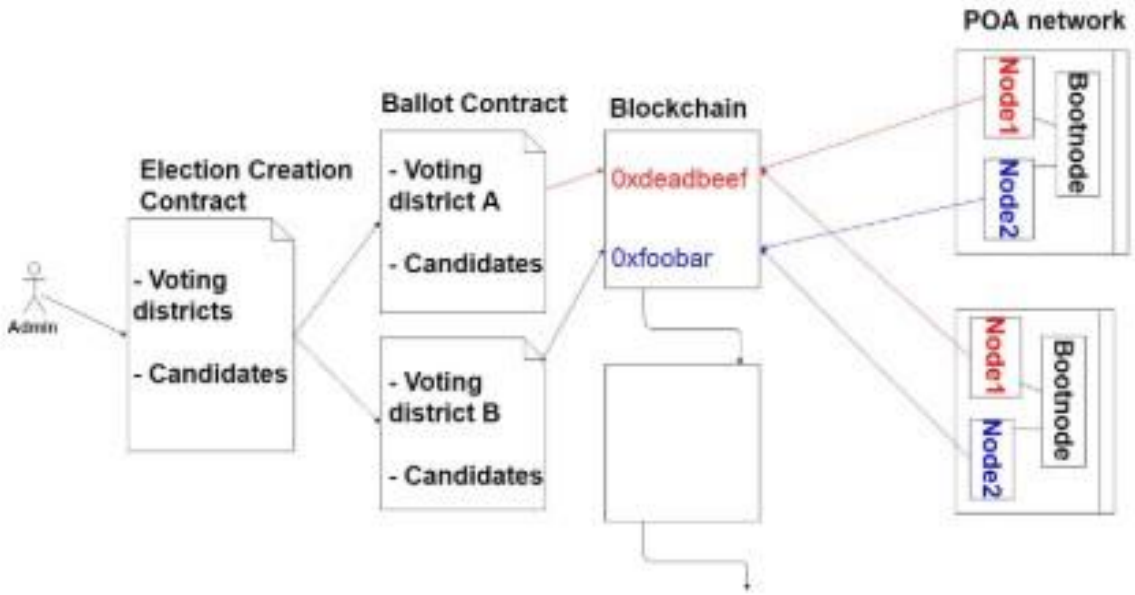


Figura 2. 10: Elecciones como contrato inteligente
Fuente: (Hjalmarsson et al., 2018)

cuando se utiliza una infraestructura de blockchain (Hjalmarsson et al., 2018).

2.9 Java

El lenguaje de programación Java fue desarrollado por Sun Microsystems a principios de los años 90. Aunque se utiliza principalmente para aplicaciones basadas en Internet, es un lenguaje sencillo, eficiente y de propósito general. Este lenguaje se diseñó originalmente para aplicaciones de

red integradas que se ejecutan en múltiples plataformas. Es interpretado, portátil y orientado a objetos. También, es extremadamente portable. Tiene un conjunto de características de seguridad que protegen a un PC que ejecuta un programa no sólo de los problemas causados por un código erróneo, sino también de los programas maliciosos (como los virus) (Austerlitz, 2003).

Su uso de código de bytes compilado permite que el intérprete (la máquina virtual) sea pequeño y eficiente (y casi tan rápido como la CPU que ejecuta el código nativo compilado). Además, este código de bytes da a Java su portabilidad: se ejecutará en cualquier JVM que esté correctamente implementada, independientemente de la configuración del hardware o del software del ordenador(Austerlitz, 2003).

2.9.1 Java Swing

Swing en Java es un conjunto de herramientas de interfaz gráfica de usuario ligera que tiene una amplia variedad de widgets para la construcción de aplicaciones basadas en ventanas optimizadas. Forma parte de JFC (Java Foundation Classes). Es independiente y tiene componentes ligeros (Waseem, 2021)

Es más fácil construir aplicaciones ya que tiene componentes GUI (Interfaz gráfica de usuario) como botones, casillas de verificación, etc. Esto es útil porque no tenemos que empezar desde cero. (Waseem, 2021).

Según (Waseem, 2021) java está compuesta por clases y por lo menos necesita una clase contenedora, la cual es llamada así por contener otros componentes. Para construir aplicaciones GUI se necesita al menos una clase contenedora. Los siguientes son los tres tipos de clases contenedoras:

- Panel - Se utiliza para organizar los componentes en una ventana
- Frame - Una ventana completamente funcional con iconos y títulos

- Dialog - Es como una ventana emergente pero no totalmente funcional como el frame

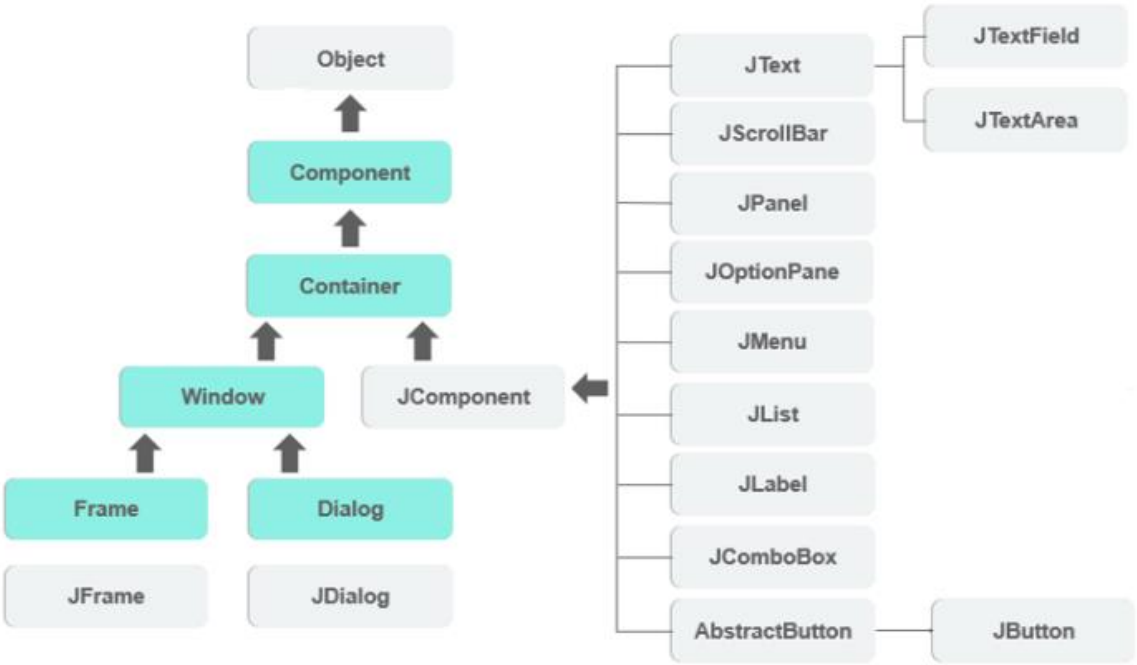


Figura 2. 11: Componentes y jerarquía de Java Swing
Fuente: (Waseem, 2021)

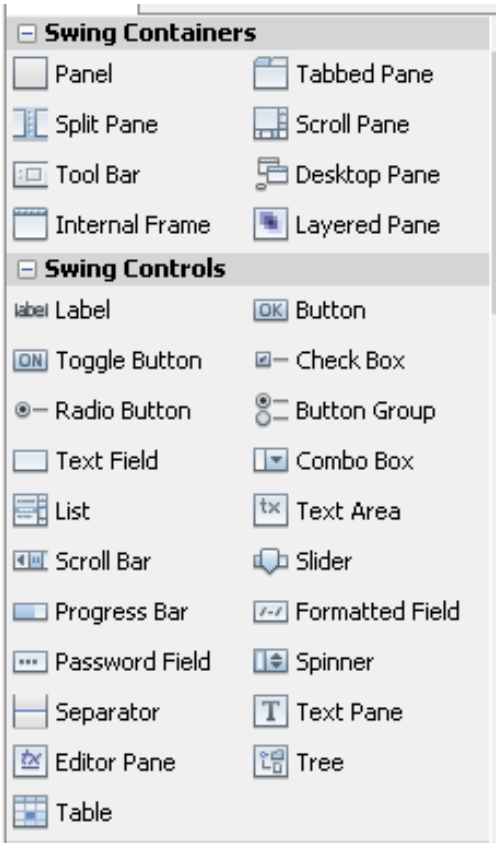


Figura 2. 12: Paleta de Java Swing
Elaborado por: Autor

Algunos de los componentes que se utilizarán para el modelado de sistema de votación son:

- JOptionPane

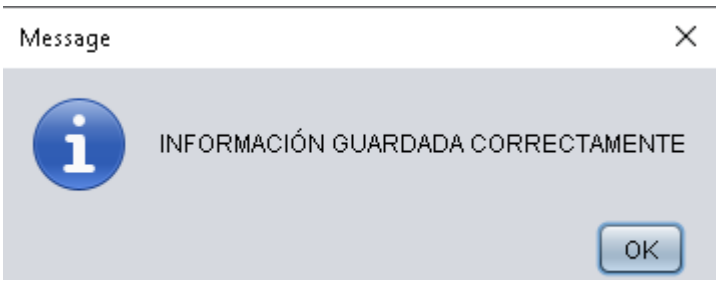


Figura 2. 13: JOptionPane
Elaborado por:Autor

- JComboBox

Figura 2. 14: Java JComboBox
Elaborado por: Autor

- JRadioButton

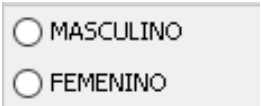


Figura 2. 15: JRadioButton
Elaborado por:Autor

2.10 Consejo Nacional Electoral (CNE)

El consejo Nacional Electoral o también conocido como CNE, surgió a partir de que la Asamblea Constituyente de Montecristi en el año 2008, decidiera agregar dos poderes más al Estado ecuatoriano, dichas funciones son la Función Electoral y la Función de Transparencia; lo que trajo consigo que la CNE fuese establecida junto con el Tribunal Contencioso Electoral (Noboa, 2015).

Como se quería reorganizar el marco administrativo del Estado, también, se creó un régimen de transición, naciendo así la CNE de Transición,

que en las primeras elecciones del 2009 estuvo a cargo de Omar Simón (Noboa, 2015).

Desde la creación de la CNE, esta institución se ha encargado de varios procesos electorales y consultas populares (Noboa, 2015) .

Figura 2. 16: Consejo Nacional Electoral (CNE)
Fuente: (Noboa, 2015)

Capítulo 3: Modelado de un sistema de votación electrónico a través de Jframe de Java Swing

3.1 Antecedentes del proyecto

El concepto del voto electrónico es algo que viene surgiendo desde hace pocos años atrás, por eso existen varias ideas para ello como el E-Voting y Remote E-Voting, pero estas tienen varios fallos como no poder autenticar la información del votante, así como autenticidad de los votos; no proteger el anonimato del voto; ataques de hackers como intercepción y modificación de papeletas; de la misma manera tiene la posibilidad de que se vea afectada la confidencialidad. Por ello, se propone hacer un sistema de votación apoyado en blockchain, debido a que con esta tecnología se puede realizar transacciones íntegras, hay confidencialidad, se permite el anonimato, entre otras características mencionadas anteriormente.

3.2 Diagramas de flujo de configuraciones del modelado de sistema de votación

3.2.1 Diagrama de la configuración de datos del ciudadano

Los ciudadanos ecuatorianos poseen datos básicos y únicos, los cuales son importantes para ser identificados en la sociedad. Por ello, para ejercer el derecho al voto, se quiere recolectar la información personal de la ciudadanía y a través de ese proceso permitir a los habitantes ejercer su derecho a elegir nuevas dignidades gubernamentales.

La cédula de ciudadanía contiene los siguientes datos: apellidos y nombres; lugar de nacimiento; fecha de nacimiento; nacionalidad; sexo; estado civil; número de cédula; instrucción; profesión/ocupación; apellidos y nombres del padre; apellidos y nombres de la madre; lugar y fecha de expedición; fecha de expiración; código dactilar; y firma de cedulado. Sin embargo, para ingresar al sistema de votación solo se requiere ingresar los datos importantes que permitan verificar que la persona de quien se ingresa la información es la que está votando.

En el diagrama de flujo se puede observar que para ingresar al sistema de votación se requiere llenar datos personales como: apellidos, nombres,

sexo, estado civil, provincia, cantón, parroquia y fecha de nacimiento; además, también se quieren la información única de la persona poseedora de la cédula de identidad, los cuales son número de identificación, su fecha de expiración y el código dactilar que se encuentra en la parte posterior del documento.

Figura 3. 1: Diagrama de flujo del sistema de votación
Elaborado por: Autor

En caso de que no se llenen todos los datos solicitados por el sistema, este tendrá un error y no podrá acceder la plataforma de votación.

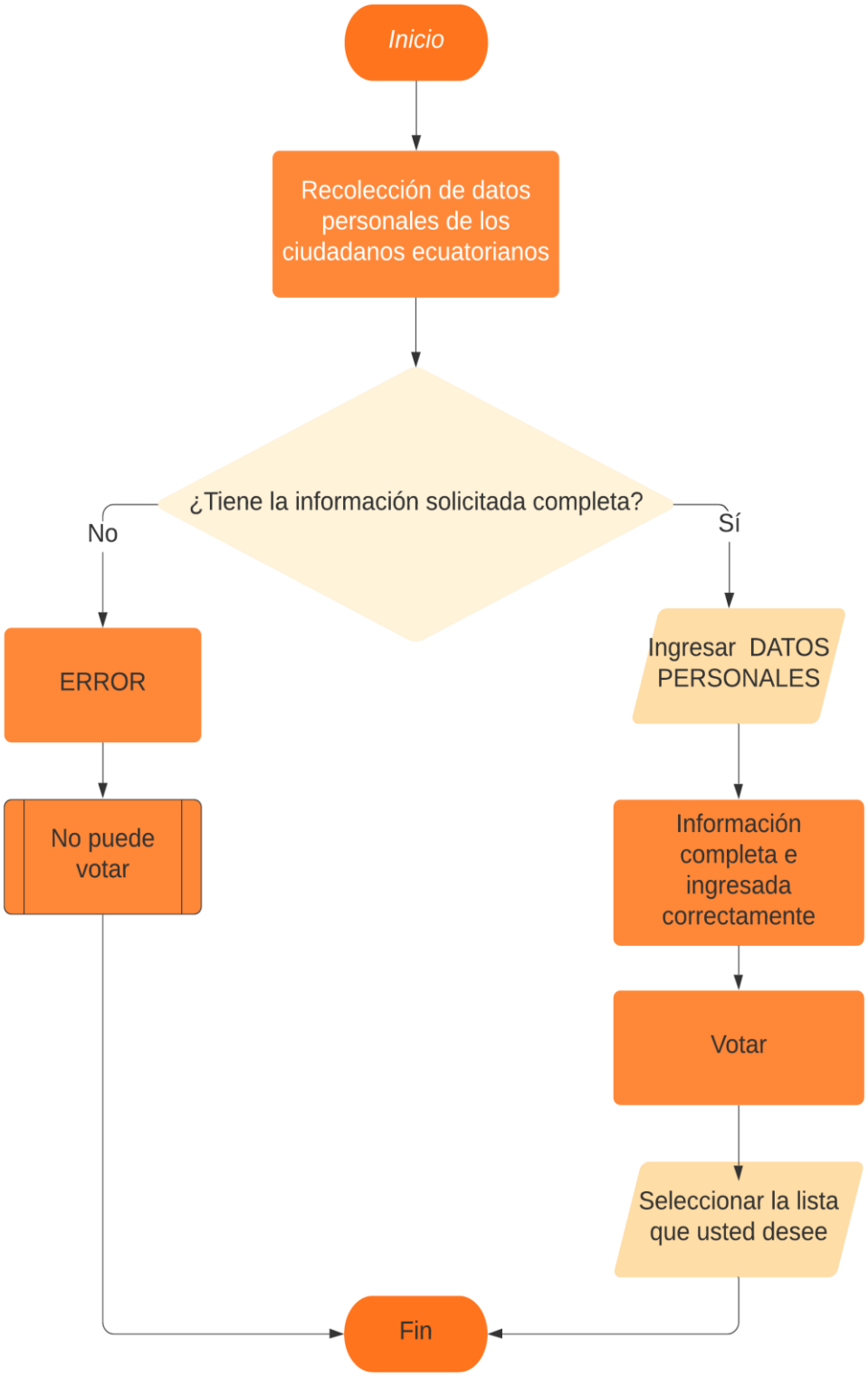


Figura 3. 2: Diagrama de flujo en donde se reporta un error por no ingresar los datos del ciudadano completos o por ingresarlos incorrectamente
Elaborado por: Autor

Tampoco se podrá acceder al sistema de votación en caso de llenar los datos personales del ciudadano de manera errónea, es decir, si se equivoca en poner la fecha de nacimiento o en escribir en algún otro campo, no podrá votar hasta que la información solicitada sea llenada correctamente.

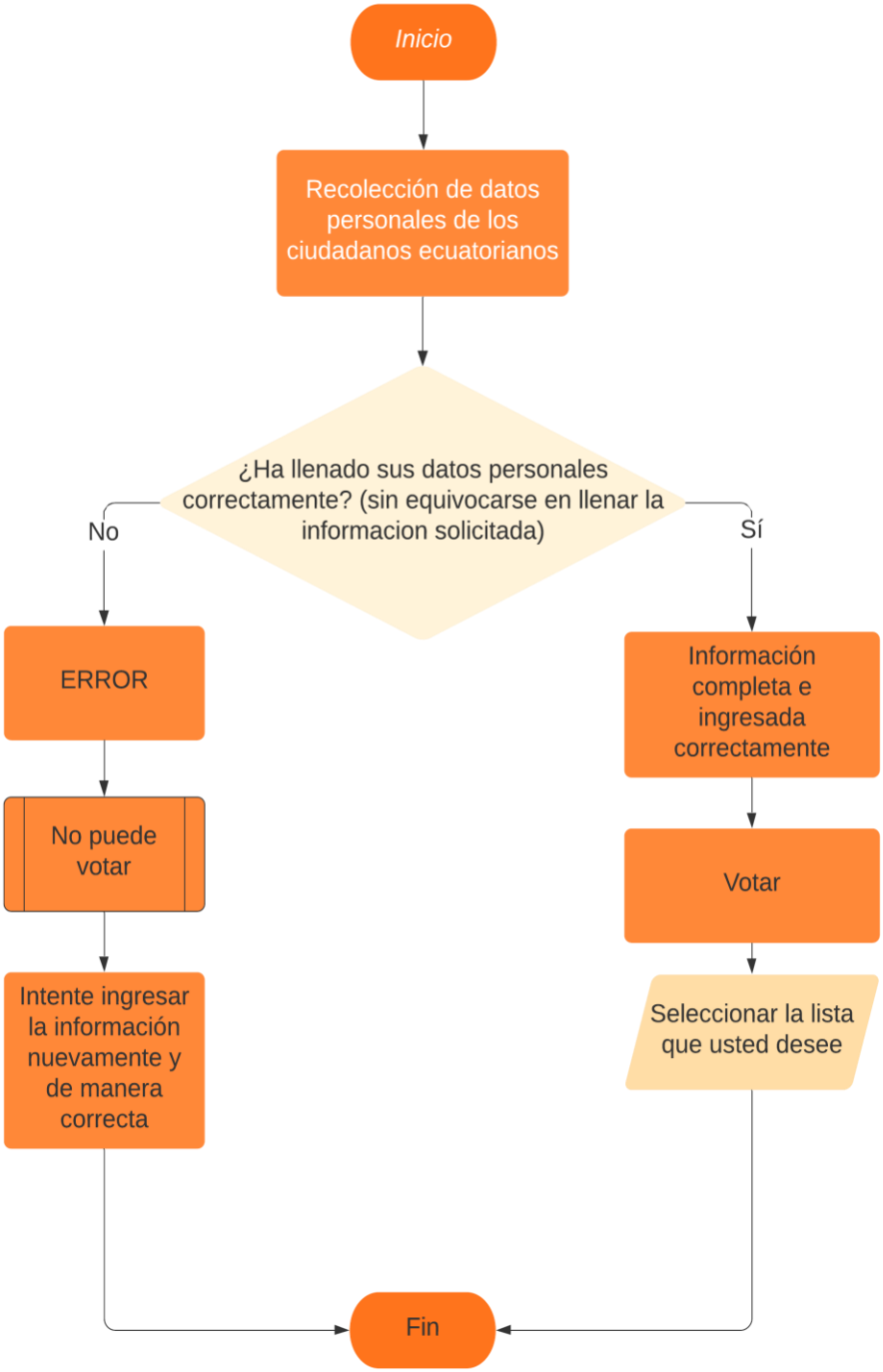


Figura 3. 3: Diagrama de flujo en donde se reporta un error por ingresar los datos del ciudadano erróneamente
Elaborado por: Autor

3.2.2 Diagrama de la configuración de los partidos o movimientos políticos de los candidatos para las elecciones electorales

En Ecuador hay varios movimientos políticos, en donde se afilian las personas y solo los más capaces (según sus criterios) son seleccionados para ser candidatos de las diferentes dignidades. Sin embargo, el ciudadano también tiene la opción de no solo elegir una de las opciones de partidos políticos, para que gobierne el Estado, sino que también, puede reservarse el voto y ejercer su derecho con diferentes alternativas, ya sea su decisión marcar la papeleta con nulo o blanco.

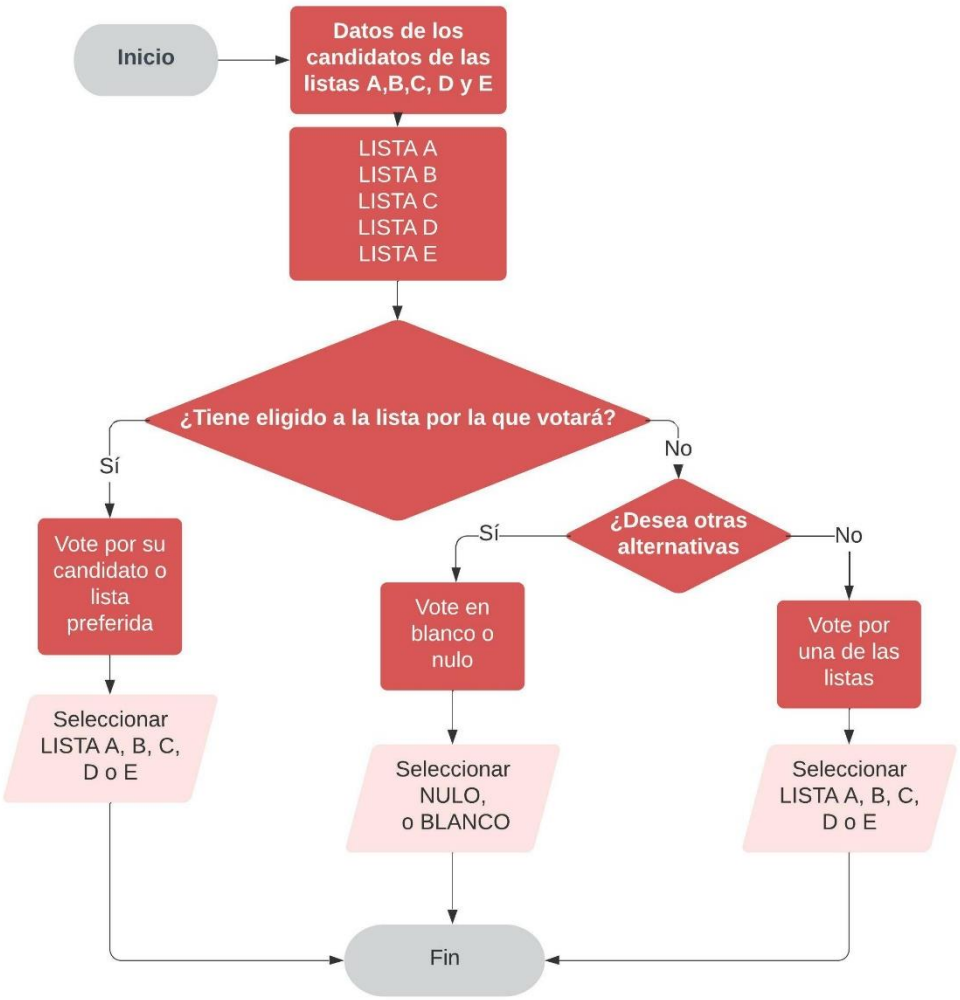


Figura 3. 4: Diagrama del sistema de votación
Elaborado por: Autor

En el diagrama se observa los movimientos o partidos políticos que están aprobadas por el CNE, y el ciudadano puede elegir entre cualquieras de los candidatos e incluso tiene otras alternativas de votación tales como el voto nulo o blanco.

3.3 Características que debería tener un sistema de votación basado en blockchain

Según (Hjalmarsson et al., 2018) después de saber las diferencias y evaluar los sistemas de voto electrónico existentes, así como también parte de los requisitos que existen para que estos funcionen de manera eficaz en los sistemas electorales, se puede decir que hay varios puntos que se pueden destacar, los cuales son requisitos viables:

- Los sistemas electorales deben de tener un método de autentificación seguro a través de la verificación de la identidad del ciudadano.
- El voto de ser permanecer en el anonimato, el sistema electoral no debe rastrear los votos hasta el respectivo votante.
- El ejercicio del voto debe ser transparente, y al mismo tiempo se debe garantizar al ciudadano de que su voto ha sido contado.
- El sistema debe garantizar al ciudadano de que ningún tercero va a modificar su voto.

3.4 Realización del modelado en Java Swing

Para realizar el modelado se usará el software de NetBeans, en la cual se puede utilizar Java Swing.

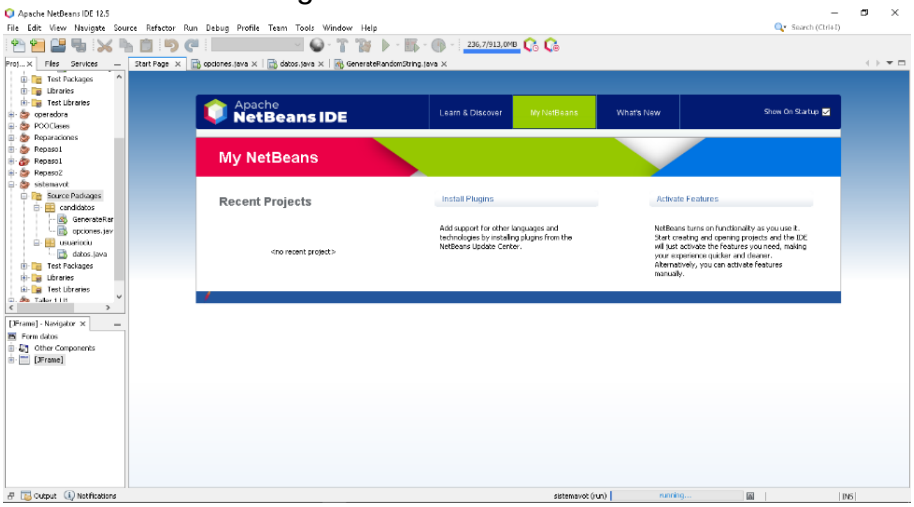


Figura 3. 5: NetBeans
Elaborado por: Autor

Se crea un nuevo proyecto en java para así comenzar a hacer el modelado.

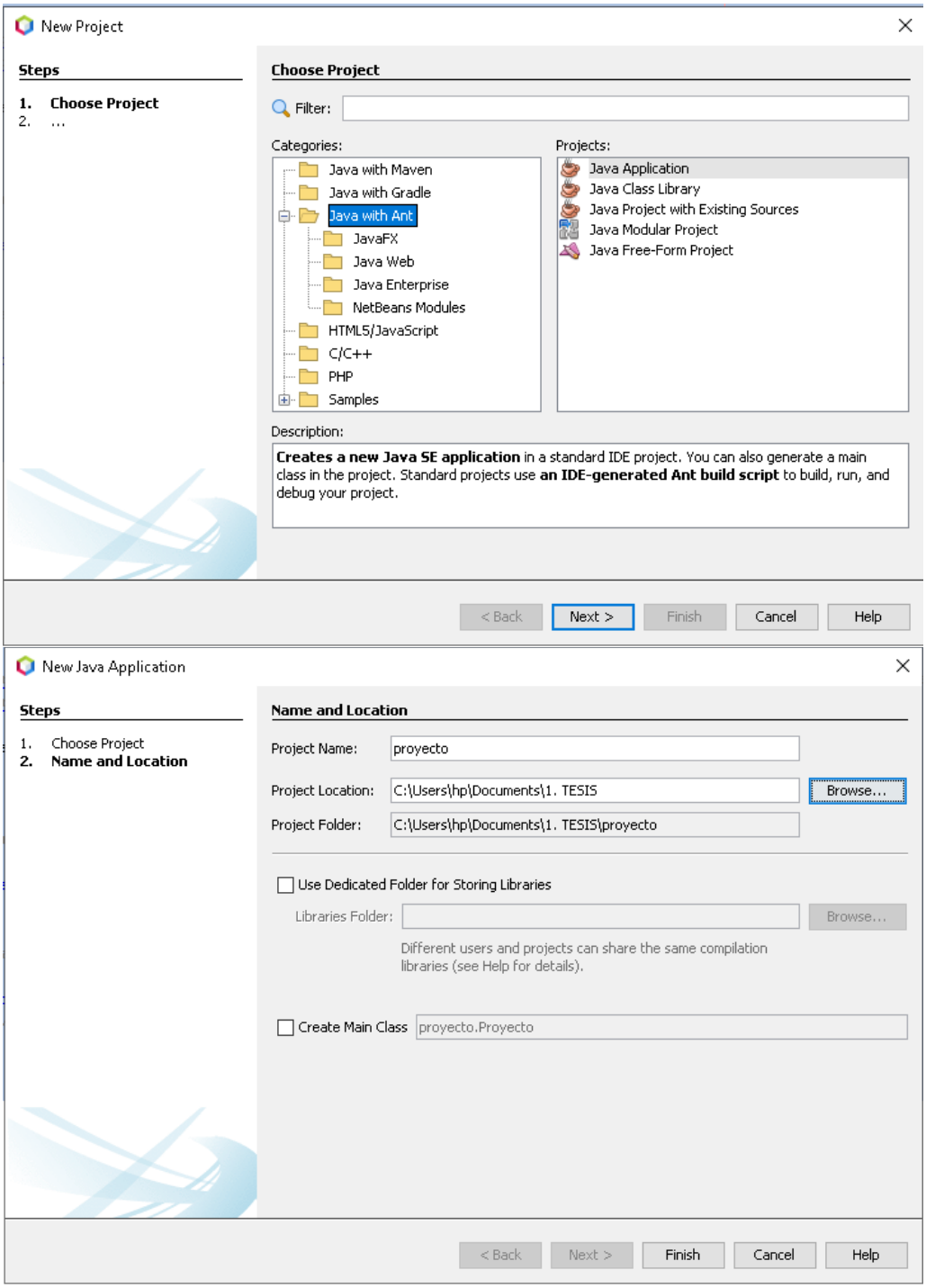


Figura 3. 6: Creación de nuevo proyecto
Elaborado por: Autor

Luego se procede a crear un nuevo paquete y el JFrame en el paquete ya existente.

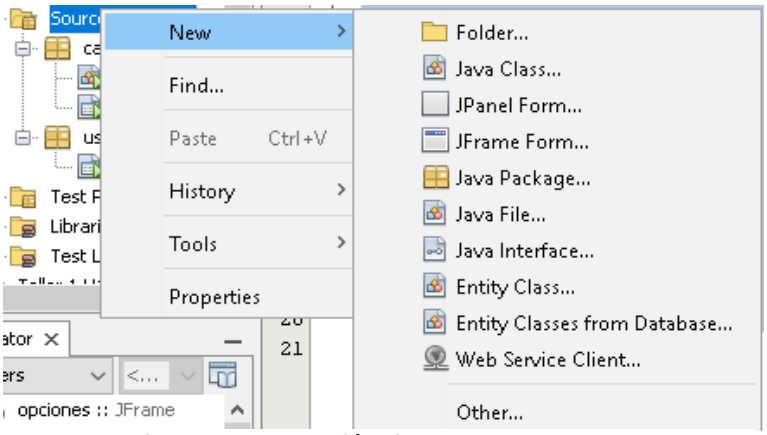


Figura 3. 7: Creación de un nuevo paquete
Elaborado por: Autor

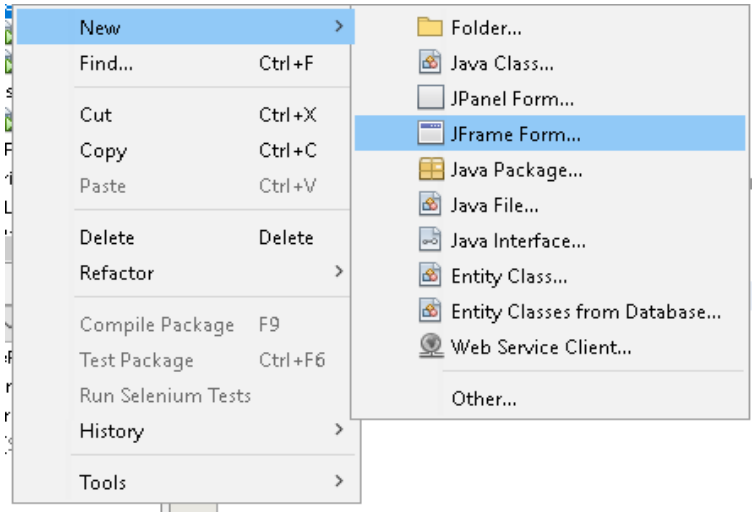


Figura 3. 8: Creación de JFrame dentro del nuevo paquete
Elaborado por: Autor

3.4.1 Modelado de la ventana que solicita los datos personales del ciudadano

Con el uso de las herramientas de la paleta como: JLabel, JButton, JRadioButton, ButtonGroup, JTextField, JComboBox, JSeparator, en donde JLabel se utiliza para escribir el texto propio del programa, en el que usuario externo no lo puede cambiar; JButton se emplea para que cuando este se accione, se muestre un mensaje a través de JOPtionPane; JRadioButton permite elegir ente varias opciones, en este caso entre masculino y femenino; ButtonGrroup deja que solo se escoja una opción de JRadioButton, es decir, que solo permite seleccionar masculino o femenino, pero no ambas al mismo tiempo; JTextField admite que el usuario pueda llenar lo que se requiere, en

este caso, sus datos personales; JComboBox muestra varias opciones y solo se puede elegir una, en este proyecto se aplica cuando se requiere la provincia de nacimiento del ciudadano y JSeparator hace que la ventana se divida en dos secciones, así como se observa entre los datos y el lugar de nacimiento. Así el código se va generando en donde se obtiene esto:

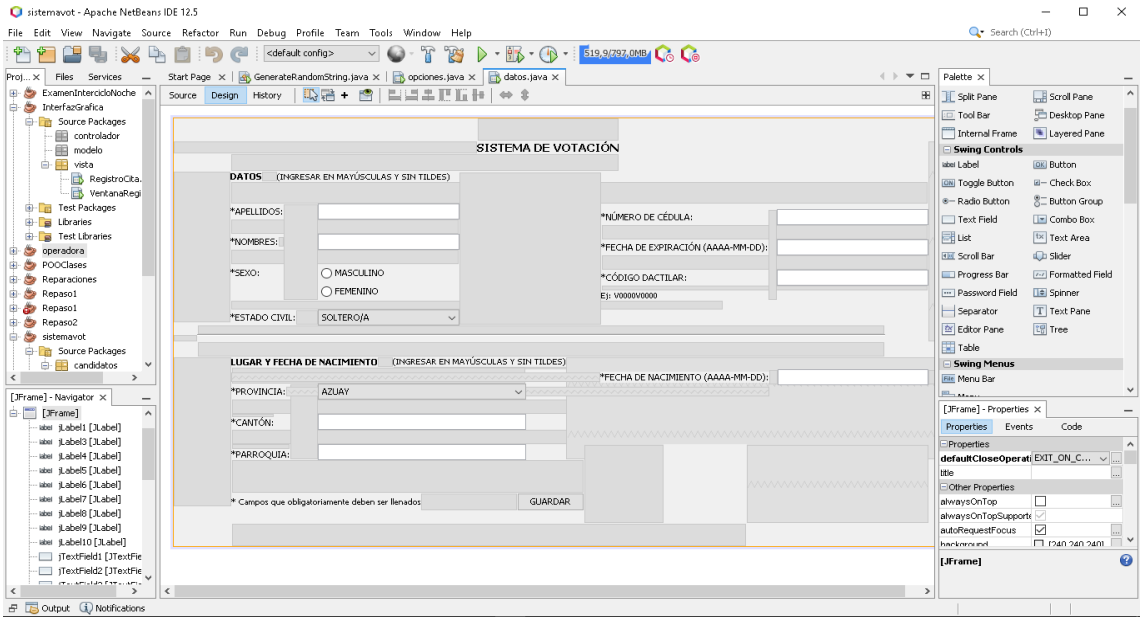


Figura 3. 9: JFrame de la ventana de los datos personales del ciudadano
Elaborado por: Autor

También, JButton (Guardar) tiene una acción agregada que cuando se ejecuta aparece un mensaje proporcionado por JOptionPane

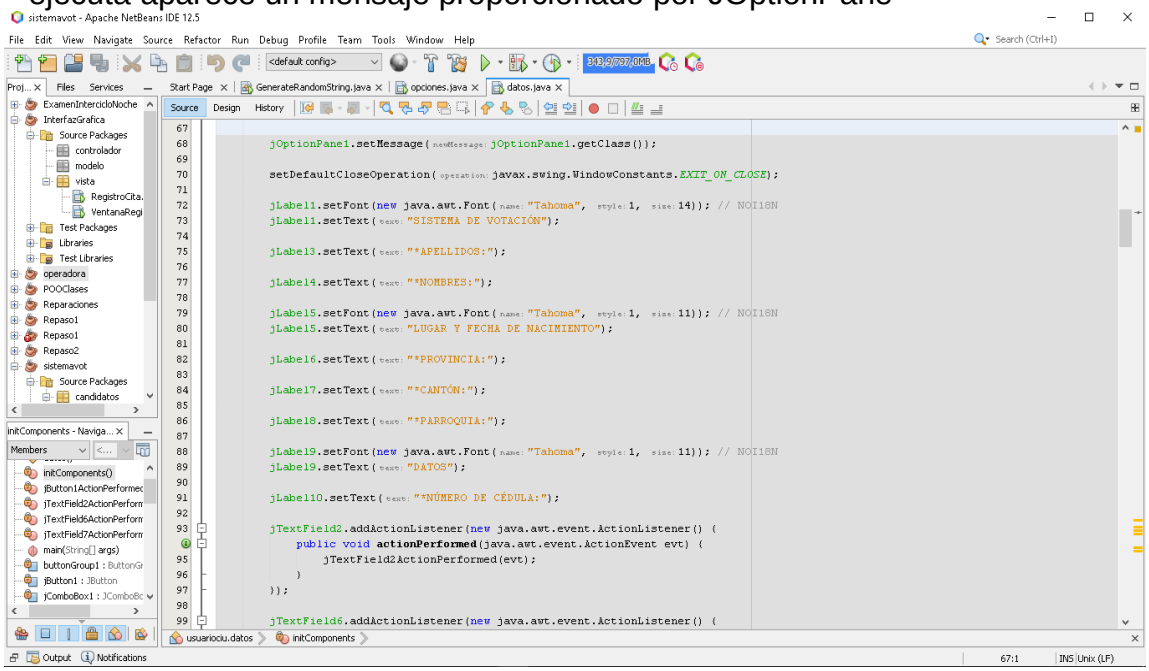


Figura 3. 10:Parte del código generado
Elaborado por: Autor

Apareciendo así un mensaje como este al presionar “Guardar”

```
private void jButton1ActionPerformed(java.awt.event.ActionEvent evt) {
    // TODO add your handling code here:
    JOptionPane.showMessageDialog (parentComponent: null, message: "INFORMACIÓN GUARDADA CORRECTAMENTE");
}
```

Figura 3. 11: Código para que aparezca el mensaje por JOptionPane
Elaborado por: Autor

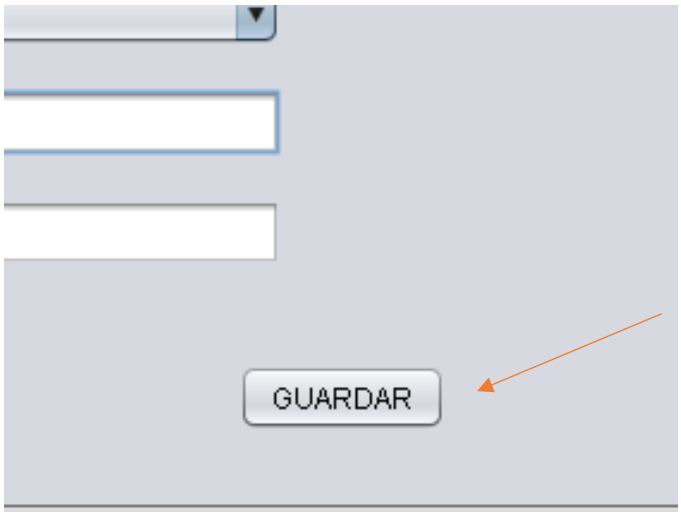


Figura 3. 12: Presionar JButton (GUARDAR)
Elaborado por: Autor

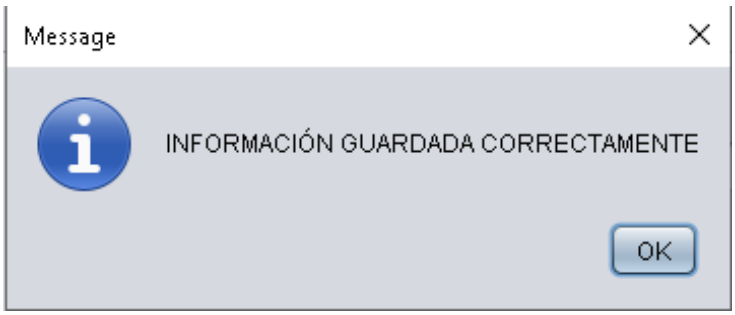


Figura 3. 13: Mensaje proporcionado por JOptionPane al presionar JButton
Elaborado por: Autor

3.4.2 Modelado de la ventana de votación

En esta ventana se usa las herramientas de la paleta como JLabel, JTable, JRadioButton, ButtonGroup, JButton, en donde JLabel se emplea para motrar el texto de la venta; JTable se usa para enseñar ordenadamente las listas y los candidatos; JRadioButton se utiliza para elegir entre las listas mostradas o para seleccionar otras alternativas; ButtonGroup permite seleccionar solo una de las opciones; JButton permite guardar el voto y al accionarlo aparece un mensaje proporcionado por JOptionPane.

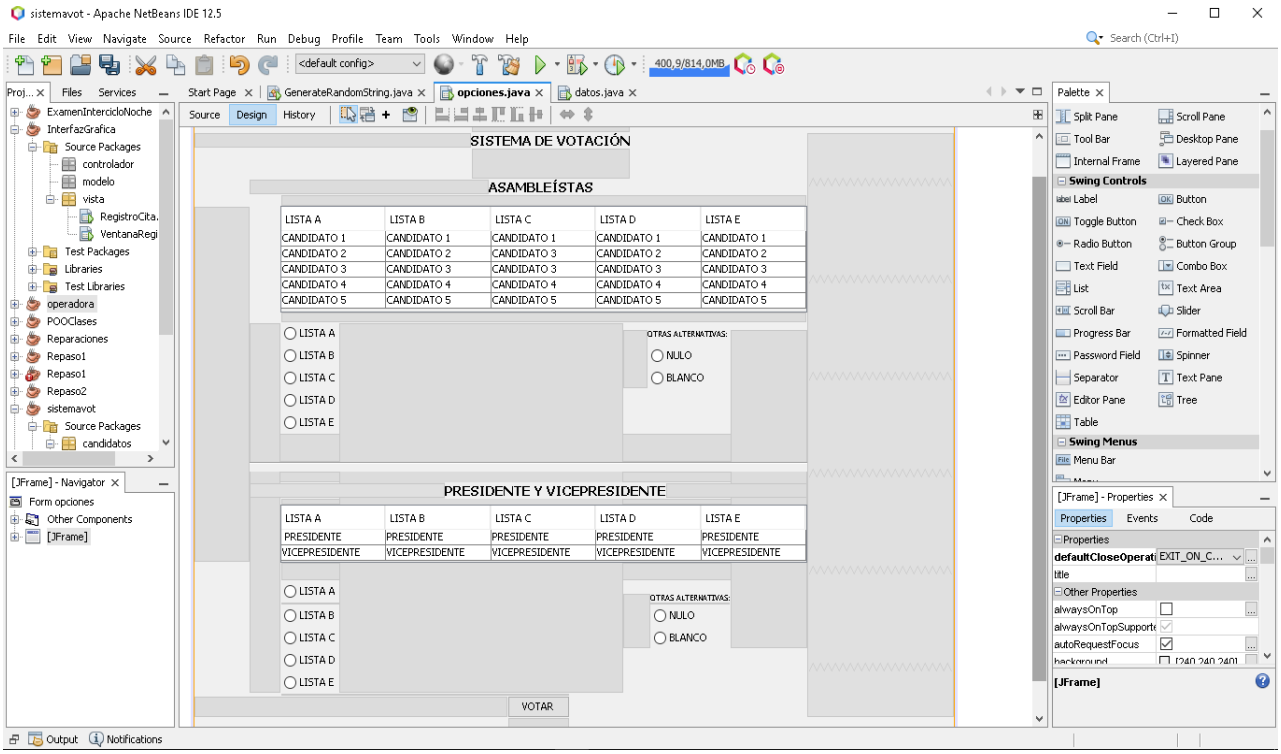


Figura 3. 14 JFrame de la ventana de votación
Elaborado por: Autor

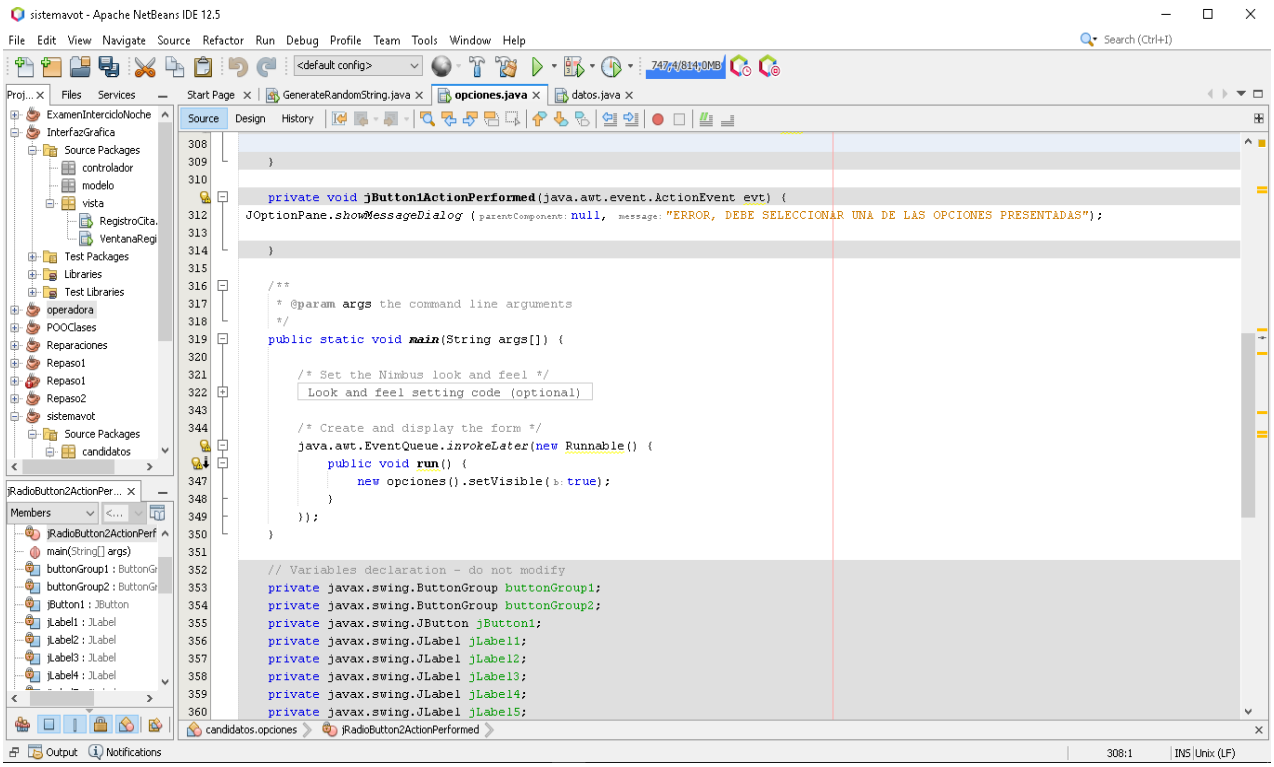


Figura 3. 15 Parte del código de la ventana de votación
Elaborado por: Autor

3.5 Simulación de un sistema de votación con Java Swing JFrame

3.5.1 Plataforma de ingresar datos de usuario

En esta parte es en donde el ciudadano debe de ingresar su información personal, es sustancial llenar los datos correctamente y completos, si no, no podrá acceder a la plataforma de votación.

Los datos que se deben proporcionar en este apartado son: apellidos; nombres; sexo; estado civil; número de cédula, su fecha de expiración, y el código dactilar; provincia, cantón, parroquia, y fecha de nacimiento; y se deben de escribir en mayúsculas, sin tildes y de manera obligatoria.

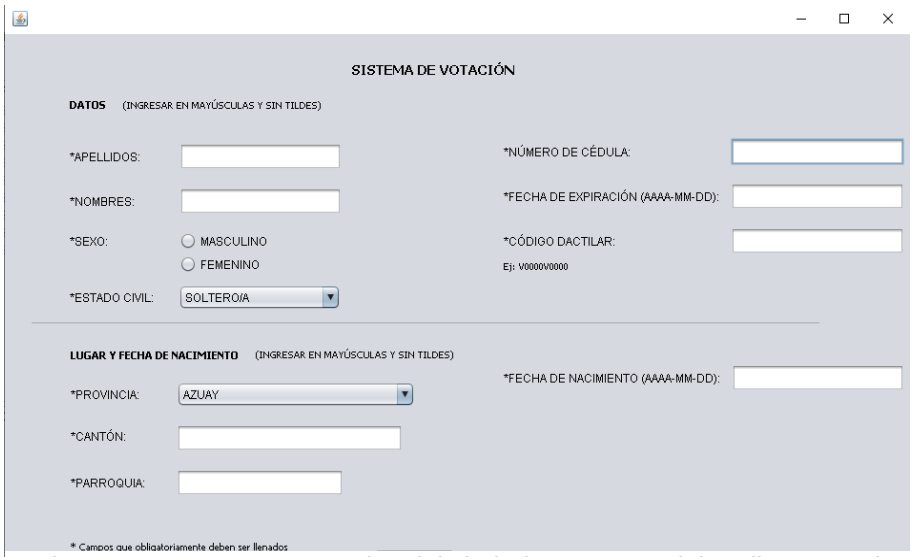


Figura 3. 17: Datos personales del ciudadano que se deben llenar en el sistema
Elaborado por: Autor

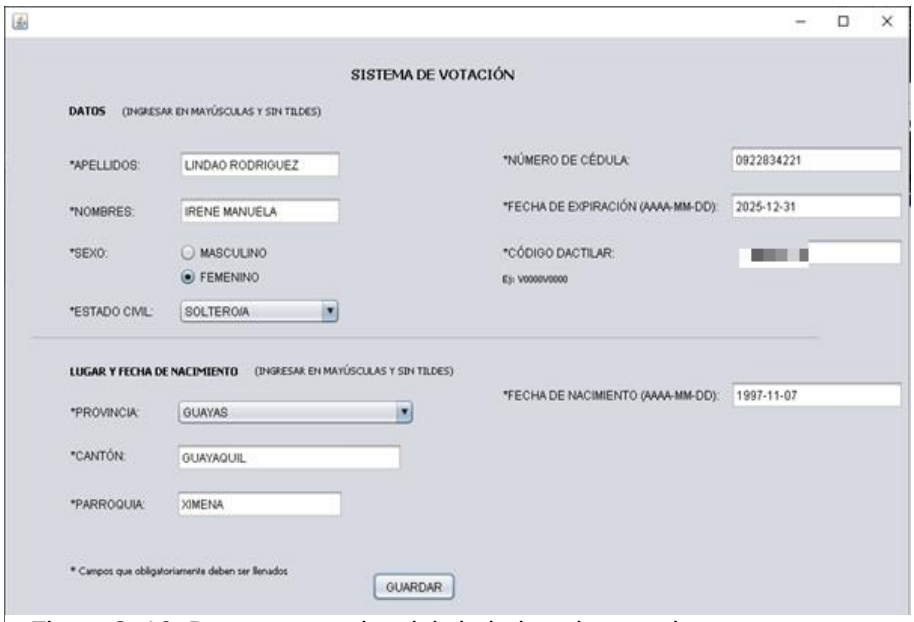


Figura 3. 16: Datos personales del ciudadano ingresados correctamente
Elaborado por: Autor

Cuando no se llena la información requerida de manera completa o si se escribe con errores, aparecerá un mensaje de error, error que se podrá corregir posteriormente.

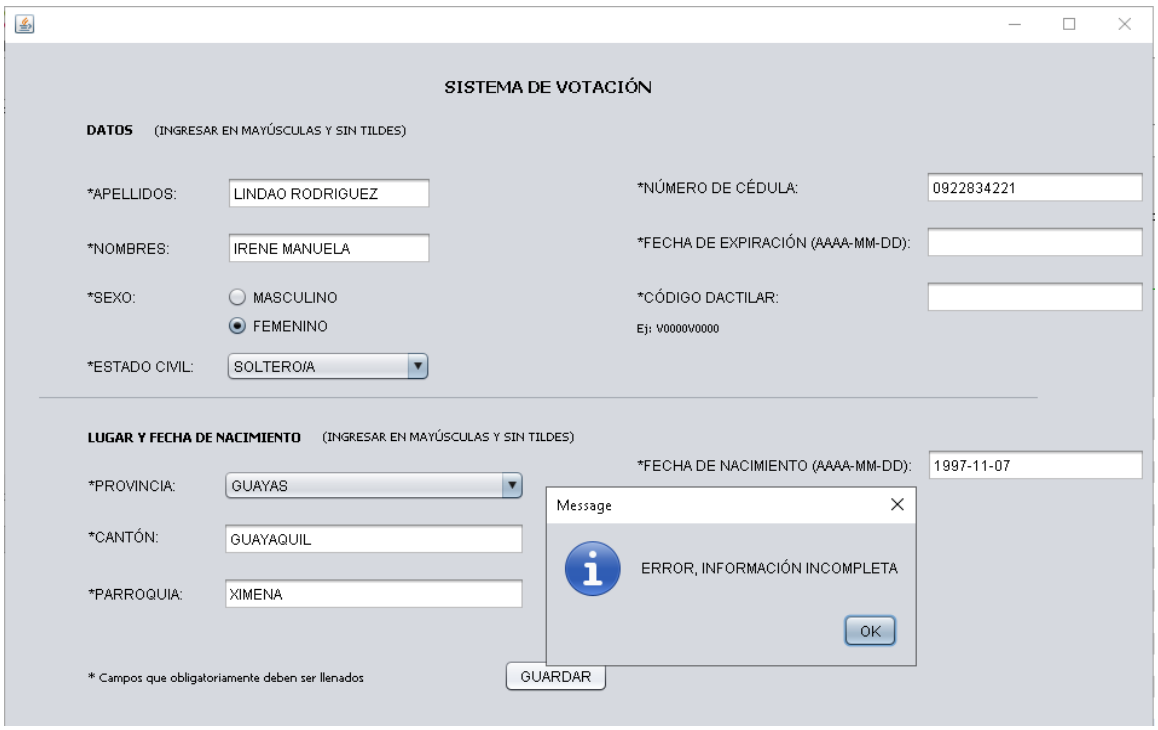


Figura 3. 18: Mensaje de error por datos incompletos
Elaborado por: Autor

Una vez realizada la respectiva corrección, ya no rebotará el mensaje de error y el sistema aceptará los datos ingresados.

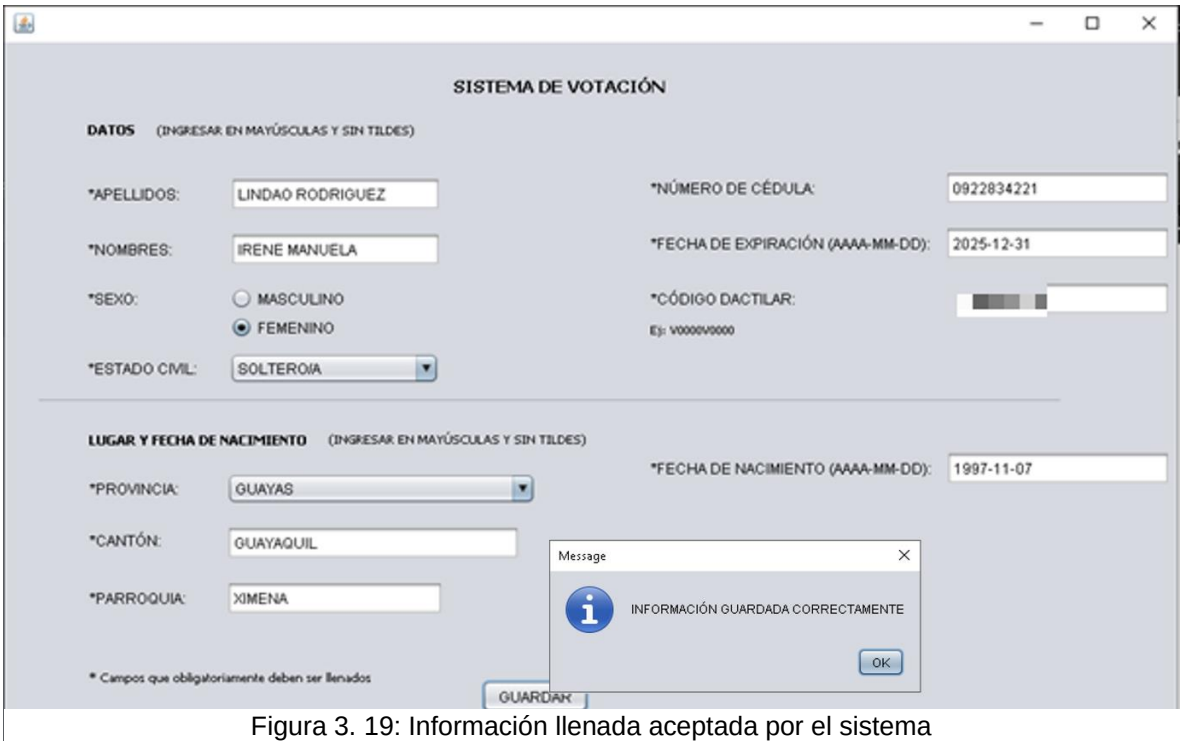


Figura 3. 19: Información llenada aceptada por el sistema
Elaborado por: Autor

3.5.2 Plataforma para votar por los diferentes movimientos políticos

Después de ingresar correctamente los datos personales del ciudadano, se accederá a una nueva ventana en donde se podrá votar por los diferentes partidos y los candidatos. En este apartado se mostrará el nombre de la lista, quienes son los candidatos de estas.

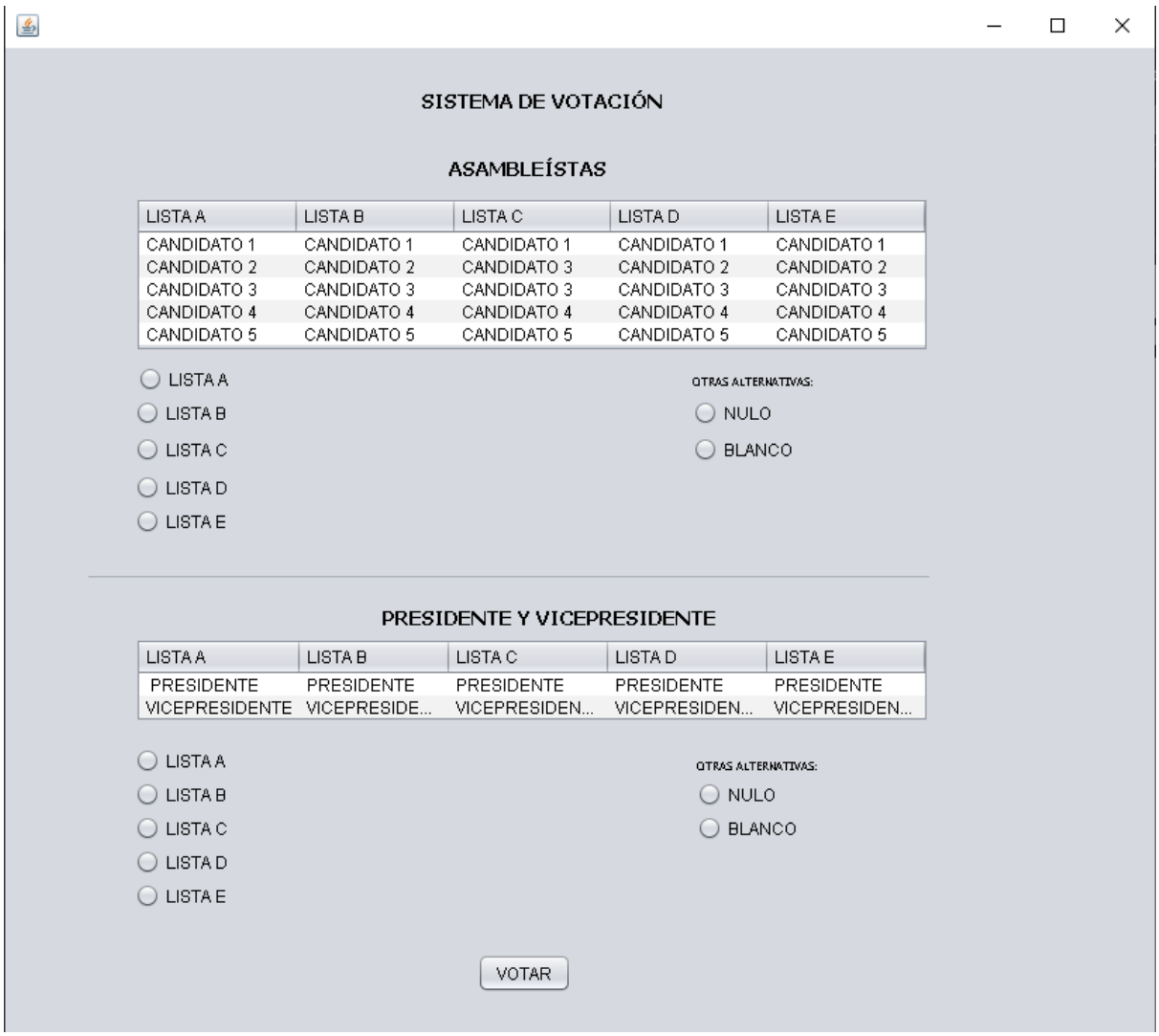


Figura 3. 20: Ventana en donde se visualizan las opciones de candidatos con sus respectivos movimientos políticos
Elaborado por: Autor

En la parte de abajo de la presentación de los candidatos, están las opciones para seleccionar por quien o por cual es la mejor opción para votar según el criterio del ciudadano. Solo se puede seleccionar una por sección, es decir, solo se puede seleccionar una opción para asambleístas o una

opción para el binomio de presidente y vicepresidente. Esto se debe a que esa es la codificación que se le ha dado al programa.

```
});
jTable2.setToolTipText( text: "");
jTable2.setCellSelectionEnabled( cellSelectionEnabled: true);
jScrollPane2.setViewportView( view: jTable2);

buttonGroup2.add( b: jRadioButton5);
jRadioButton5.setText( text: "LISTA A");

buttonGroup2.add( b: jRadioButton6);
jRadioButton6.setText( text: "LISTA B");

buttonGroup2.add( b: jRadioButton7);
jRadioButton7.setText( text: "LISTA C");

buttonGroup2.add( b: jRadioButton8);
jRadioButton8.setText( text: "LISTA D");

buttonGroup2.add( b: jRadioButton9);
jRadioButton9.setText( text: "LISTA E");

buttonGroup2.add( b: jRadioButton13);
jRadioButton13.setText( text: "NULO");

buttonGroup2.add( b: jRadioButton14);
jRadioButton14.setText( text: "BLANCO");
```

Figura 3. 21: Parte de la codificación realizada en Netbeans para poder seleccionar una sola opción
Elaborado por: Autor

Después se seleccionar la mejor opción según el criterio del ciudadano, el podrá accionar el botón de votar y le aparecerá un mensaje diciendo que su voto ha sido procesado. El ciudadano puede votar por la lista que desee, así como también puede escoger otras alternativas como el voto nulo o blanco.

En caso de que el ciudadano no seleccione ninguna opción en el panel, se mostrará una ventana que le indicará que tiene que seleccionar alguna de las opciones propuestas.

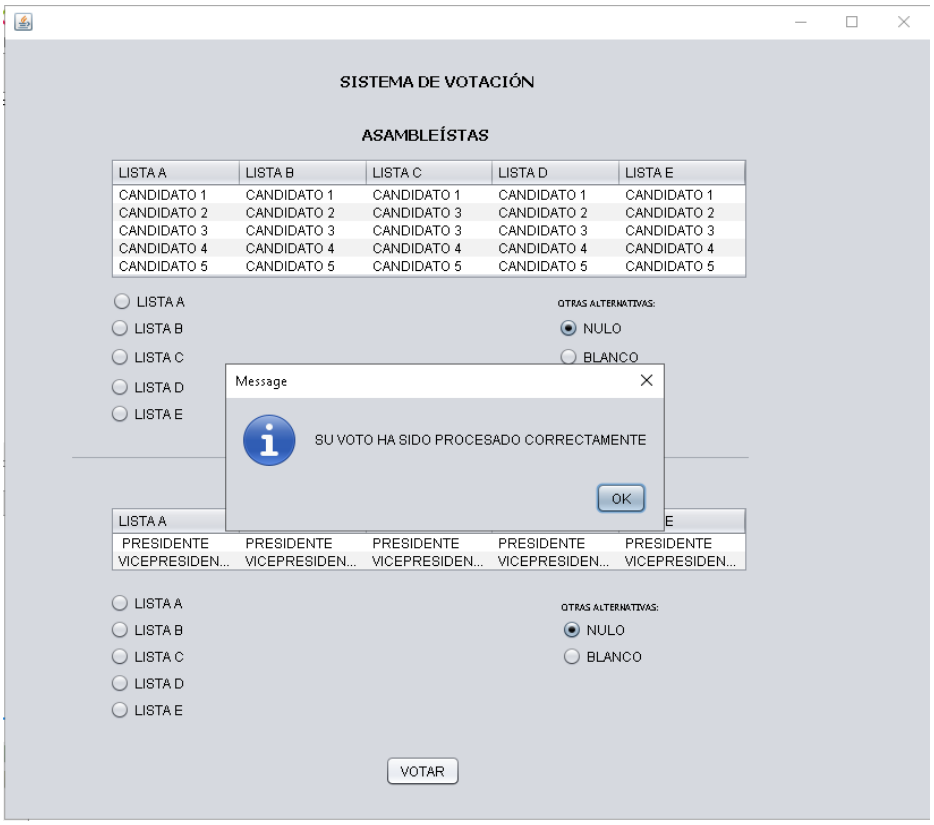


Figura 3. 23: El voto del ciudadano ha sido procesado correctamente
Elaborado por: Autor

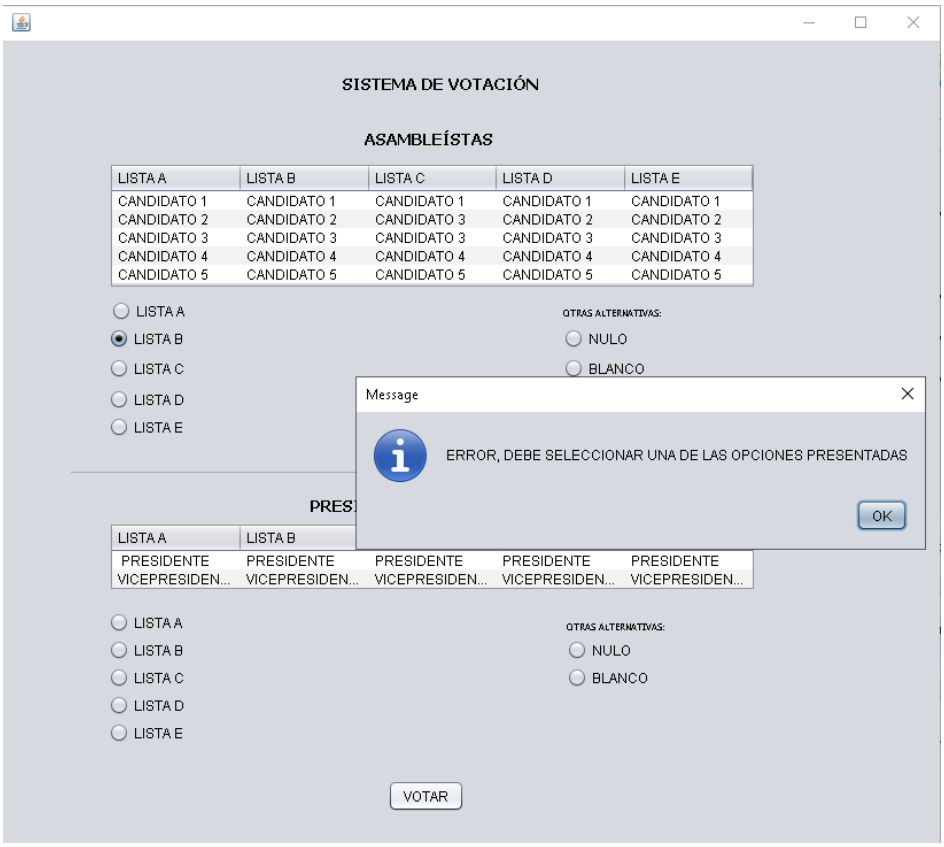


Figura 3. 22: Error al no seleccionar ninguna lista en el binomio presidencial
Elaborado por: Autor

3.6 Java y Blockchain

3.6.1 Seguridad mediante números y letras random

Blockchain ofrece seguridad y no solo eso, sino también una de las características más importantes que existen sobre el ejercicio al voto y es que permite el anonimato. Sin embargo, es predecible que muchas personas estén en contra de este sistema porque van a sentir inseguridad acerca de que su voto es secreto o no, ahí se introduce Java, y es que este lenguaje tiene una función que se importa llamada “random”, la cual permite mostrar números aleatorios y si se combina con “String” saldrá una variedad de números y letras. Estas características sirven para darle la posibilidad al ciudadano de rastrear su voto y seguir siendo anónimo. Seria generada después de votar y la persona podría ver si ya procesaron su voto anónimo.

```
Sú código es l0q34lbeiThcZxwkF4k3MrcJPQKqaYQltowlT9CQz44xjXs23WTlNbx
BUILD SUCCESSFUL (total time: 2 seconds)
```

Figura 3. 24: Ejemplo de un código entregado para rastrear el voto
Elaborado por: Autor

Se pretende que exista una plataforma en donde el ciudadano pueda ingresar el código que le han otorgado para ver si su voto ha sido procesado, manteniendo así su anonimato y teniendo la seguridad de que su voto no fue alterado.

3.6.2 Base de datos

Como se ha mencionado en el capítulo 2, blockchain es ideal para la realización de base de datos, esta base datos con blockchain, cumpliría con la función de tener a los ciudadanos registrados en ellas, permitiendo el acceso al sistema de votación a las personas que son mayores de edad, sin la necesidad de obtener la aprobación de algún moderador, porque su registro ya está en el sistema y al momento de escribir sus datos, el sistema detectara automáticamente si están correctos o no.

Capítulo 4: Conclusiones y recomendaciones

4.1 Conclusiones

- La tecnología Blockchain es nueva, por lo tanto, hay mucho que explotar de ella como el posible hecho de hacer un sistema de votación basado en la seguridad de esta. En donde la cadena de bloques tendrá participación tanto en el área de seguridad brindando anonimato, integridad y confianza, así como en la base de datos personales de los ciudadanos.
- Los diagramas de flujo realizados para obtener una idea de lo que se debe llenar y/ o solicitar el sistema de votación, reflejan datos básicos de cualquier ciudadano, así como también como seria el ingreso del voto.
- Se logró modelar la vista y simular un sistema de votación apoyado en la seguridad que ofrece la tecnología blockchain, a través la herramienta JFrame proporcionada por Java Swing, para que los ciudadanos ecuatorianos puedan ejercer el voto desde sus hogares.

4.2 Recomendaciones

- Pasar del modelado a la aplicación e implementación para así mejorar el sistema de votación actual existente en Ecuador, evitar las aglomeraciones y ofrecer a los que no pueden acceder su derecho al voto.
- Se debe dar mantenimiento al sistema de votación y actualizar la base de datos de blockchain regularmente, para que los que van cumpliendo la mayoría de edad, puedan ejercer su voto.
- El voto electrónico debe de respetar los principios democráticos establecidos en la Constitución actual de la Republica del Ecuador, la cual afirma que el voto es personal, obligatorio y secreto.

BIBLIOGRAFÍA

Austerlitz, H. (2003). Computer Programming Languages. In *Data Acquisition Techniques Using PCs (Second Edition)* (pp. 317–323).

Braun, N. (2007). *E-voting and external voting*.

Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018). Blockchain-Based E-Voting System. *IEEE International Conference on Cloud Computing, CLOUD*.

Le, D., Kumar, R., Mishra, B. K., Khari, M., & Chatterjee, J. M. (2019). Cyber Security in Parallel and Distributed Computing. In *Cyber Security in Parallel and Distributed Computing*.

Rennock, M. J. W., Cohn, A., & Butcher, J. R. (2018). Blockchain Technology Regulatory and Investigations. *The Journal Litigation*.

Saghiri, A. M. (2019). Advanc-ed Applications of Blockchain Technology. In *Blockchain for Big Data*. https://doi.org/10.1201/9781003201670-5

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys*, *52*(3). https://doi.org/10.1145/3316481

Bharathan, V. (2020). Blockchain Was Born 20 Years Before Bitcoin. *Forbes*.

Noboa, A. (2015). La historia del CNE desde sus inicios en 2008. *El comercio*.

Waseem, M. (2021). *Swing In Java : Know How To Create GUI With Examples.* Obtenido de edureka: https://www.edureka.co/blog/java-swing/

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Lindao Rodriguez, Irene Manuela** con C.C: # 092283422-1 autor del Trabajo de Titulación: **Modelado de un sistema de votación electrónico basado en la tecnología blockchain a través de JFrame de Java Swing** previo a la obtención del título de **INGENIERA EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 7 de marzo del 2022

f. _____

Nombre: Lindao Rodriguez, Irene Manuela

C.C: 0922834221

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Modelado de un sistema de votación electrónico basado en la tecnología blockchain a través de JFrame de Java Swing		
AUTOR(ES)	Lindao Rodriguez, Irene Manuela		
REVISOR(ES)/TUTOR(ES)	Ing. Suarez Murillo, Efrain Oswaldo		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniera en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	7 de marzo del 2022	**No. DE PÁGINAS:**	47
ÁREAS TEMÁTICAS:	Seguridad y blockchain		
PALABRAS CLAVES/ KEYWORDS:	Blockchain, Seguridad, Java, Votación, Modelado		

RESUMEN/ABSTRACT (150-250 palabras):

Para el desarrollo del presente trabajo de titulación, se optó por usar Java swing en conjunto con JFrame en el software NetBeans, para modelar un sistema de votación apoyado en la nueva tecnología llamada Blockchain la cual ofrece seguridad al ciudadano de que su decisión no se podrá alterar ni modificar; anonimato para los votantes; y base de datos en donde estarán registrados quienes pueden ejercer su derecho al voto; estas cualidades son fundamentales para el desarrollo de este tipo de sistemas, por ello, se realizó un modelo de un sistema de votación, en dónde los ciudadanos ecuatorianos pueden acceder al voto desde la comodidad de su hogar, pero primero deben identificarse escribiendo sus datos personales, después de escribirlos correctamente, se podrá acceder a la ventana dónde aparecerá los diferentes partidos o movimientos políticos y candidatos aprobados por la CNE, y de esa manera podrá hacer su ejercicio al voto. Así, se podrá evitar aglomeraciones y contratiempos que surgen al momento de votar, cuando las personas se trasladan a su recinto electoral.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593994622288	E-mail: irenelindaorod@gmail.com
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Palacios Meléndez, Edwin Fernando **Teléfono:** +593-9-67608298 **E-mail:** edwin.palacios@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	