Propuesta de Diseño de un Prototipo de Red Blockchain Aplicado a un Ejercicio Electoral a Nivel Colombia, Midiendo Impactos y Beneficios.

Trabajo de Grado para optar al grado de Ingeniero de Telecomunicaciones

OSCAR ALEXANDER SANABRIA BAQUERO

Director:

Ing. Fernando Prieto Bustamante

UNIVERSIDAD SANTO TOMAS

FACULTAD DE INGENIERIA DE TELECOMUNICACIONES

PREGRADO EN INGENIERIA DE TELECOMUNICACIONES

BOGOTÁ, 2021

Este trabajo de grado el cual es el cierre de mi pregrado como profesional me permite crecer como persona, el camino no ha sido fácil, pero con la ayuda primeramente de Dios ha sido posible. Este logro tan importante para mi vida se lo dedico a mis padres Manuel Sanabria y Clara Baquero que al igual que dos personas que ya no están entre nosotros siempre confiaron en mí.

Pedro Pablo Baquero Cagua quien fue ese abuelo que me dio la mano cuando más la necesitaba y me decía que si se podía y a quien le debo mucho de lo que estoy logrando en este momento, sé que lo hacía con amor porque confiaba en mí y quería verme ser un gran hombre, a mi padrino Álvaro Baquero Villalba quien me decía que si era para estudiar y cumplir mis sueños contara con él, y así fue. Ellos no me pueden acompañar ni escuchar esta dedicatoria, pero desde donde están les hago saber que este logro no es solo mío, es un logro también de ustedes y ¡dedicado a ustedes!

Recuerdo la frase de mi abuelo “Estudie mijo para ser alguien en la vida y llegar lejos y acuérdese que vinimos a este mundo para servir y no ser servidos”

Agradecimientos

A Dios principalmente por su bendición y permitir que este logro se cumpliera. Al ingeniero Fernando Prieto Bustamante por su apoyo, confianza y acompañamiento.

A mis padres Clara Inés Baquero y Manuel Sanabria por su amor, confianza y apoyo. A mi hermano por su ayuda, a mi amado Abuelo Pedro Pablo Baquero, quien fue un motor principal con su apoyo, y quien me entrego todo sin pedir nada a cambio, confianza, palabras y ejemplo, a mi padrino Álvaro Baquero quien no dudo un momento en ayudarme y a mi madrina Blanca Graciela Baquero quien ha sido mi segunda madre y me apoyo desde siempre.

A mis amigos y personas especiales que en su momento me dieron su mano y confiaron en mí, muchas gracias, sin la ayuda de ustedes tampoco hubiera sido posible.

Por último, a la facultad de ingeniería de Telecomunicaciones, resaltando la visión Tomasina, a los docentes y directivos por compartir sus conocimientos y por las experiencias compartidas.

Tabla de Contenido

Tabla de Ilustraciones

Índice de Tablas

Resumen

En el presente proyecto de grado se hace énfasis principalmente en la tecnología Blockchain haciendo énfasis en la información básica, incluyendo su funcionamiento y un estudio completo de uno de los usos más importantes de esta tecnología como las elecciones presidenciales. En este documento se hará énfasis en su gestión a nivel nacional. El diseño de la red tiene una gran escalabilidad debido a que se cuenta con acceso a las votaciones de alrededor de 40 millones de personas y su equivalente para una implementación de red al cubrimiento del 100% de los usuarios a nivel nacional, además de los ciudadanos que se encuentren en el exterior también contaran con la opción de votar; se tiene claro que es un método totalmente diferente al medio de votación tradicional.

En el presente proyecto se explican los tres métodos de votación más importantes en el mundo haciendo énfasis en sus ventajas y desventajas, así mismo los países que usan estos métodos de votación y comparándolos con el fin de concretar los beneficios de aplicar un método de votación con la tecnología blockchain en nuestro país.

Todo método de votación cuenta con una parte importante de gestión, procesos previos y posteriores, en los cuales se explicará con detalle la gestión, fases y etapas que se deben cumplir, la mejor forma de realizarse y como se relaciona y complementa con la solución técnica en un solo sistema. El capítulo de esta tesis del diseño de la gestión de las votaciones y el capítulo de la solución técnica se relacionan para hacer un sistema completo de votación basado en la tecnología Blockchain, el cual se propone como alternativa tecnológica a desarrollar y contemplar para unas elecciones a nivel nacional, en donde no se afecte la estructura de las elecciones, y siguiendo los derechos y deberes que se reglamentan en la constitución del país, así mismo resaltando y respetando las características de una votación, como el voto secreto y conocimiento de resultados al final de las elecciones, así mismo aportando nuevas características con este sistema como la transparencia, trazabilidad, privacidad, etc.

Todo este análisis técnico se acompañará de un análisis financiero del coste de la solución e implementación. Por servicio, seguridad y beneficios, se escoge y se realiza el análisis de coste sobre AWS, es decir la implementación de este sistema de votación y el análisis financiero de este sistema se realiza sobre AWS. Teniendo en cuenta todo lo anterior y lo nueva que es la tecnología *Core* para el desarrollo de esta tesis que como se ha nombrado es blockchain se recomiendan puntos importantes a tener en cuenta para que todo el sistema como está pensado sea exitoso.

Abstract

In this degree project the emphasis is mainly on blockchain technology with an emphasis on basic information, including its operation and a complete study of one of the most important uses of this technology, such as the presidential elections. This document will emphasize its management at the national level. The design of the network has a great scalability due to the fact that there is access to voting by around 40 million people and its equivalent for a network implementation to cover 100% of users nationwide, in addition to citizens. Those who are abroad will also have the option to vote; it is clear that it is a totally different method from the traditional means of voting.

This project explains the 3 most important voting methods in the world, emphasizing their advantages and disadvantages, as well as the countries that use these voting methods and comparing the 3 methods in order to specify the benefits of applying a method. Voting with blockchain technology in our country.

Every voting method has an important part of management, prior and subsequent processes, in which the management, phases and stages that must be met, the best way to carry it out, and how it relates to and complements the technical solution will be explained in detail. In a single system. The chapter of this thesis on the design of voting management and the chapter on the technical solution are related to make a complete voting system based on blockchain technology, which is proposed as a technological alternative to develop and contemplate for elections to national level, where the structure of the elections is not affected, and following the rights and duties that are regulated in the country's constitution, also highlighting and respecting the characteristics of a vote, such as secret ballot and knowledge of the results at the end elections, also providing new features with this system such as transparency, traceability, privacy, etc.

All this technical analysis will be accompanied by a financial analysis of the cost of the solution and implementation. For service, security and benefits, the cost analysis is chosen and performed on AWS, that is, the implementation of this voting system and the financial analysis of this system is performed on AWS. Taking into account all of the above and how new the core technology is for the development of this thesis, which, as it has been named, is blockchain, important points are recommended to take into account so that the entire system as it is intended is successful.

Introducción

Durante mucho tiempo en Colombia las elecciones presidenciales se han desarrollado de forma tradicional, por muchos años las personas solo han conocido una forma de votar, este método de votación tiene sus ventajas, pero también tiene desventajas las cuales permiten tener sobre la mesa o contemplar nuevas opciones y sistemas de votación que cumplan con los reglamentos de la constitución y que se ajusten a los tiempos actuales.

Desde hace unos años atrás nace una tecnología disruptiva y con mucho potencial, se conoce como la tecnología del futuro y la cual viene a cambiar muchas cosas de cómo se conocen actualmente, entre esas los sistemas de votación actuales, y más que a cambiar, la tecnología Blockchain llega a ser un complemento y aportar en la evolución de los sistemas electorales actuales, las ventajas que aporta esta tecnología son muchas, entre ellas la seguridad de la información que se maneja, las características propias del blockchain como la transparencia e inmutabilidad hacen que para un sistema de votación se adapte perfectamente.

Aparte de conocer la tecnología también se debe conocer el sistema electoral actual y como está reglamentado, con esta información el análisis a desarrollar es completo con el fin de estudiar la posibilidad de a futuro implementar un sistema electoral basado en blockchain en Colombia. Se desarrolla un análisis informativo de la tecnología, de gestión del sistema electoral, técnico y funcionamiento del sistema, costos de la solución, y por ultimo recomendaciones para que el uso del sistema que se plantea tenga el menor impacto posible, cumpla y supere con las expectativas que se tiene en el aporte de la tecnología blockchain para los sistemas electorales.

El análisis que se realiza de la tecnología Blockchain es completo porque abarca desde la historia de la tecnología, funcionamiento, ventajas y desventajas como su uso actual en el mundo en especial en el ámbito electoral, y se detalla en como funcionaria todo un sistema electoral para Colombia basado en la tecnología blockchain, conociendo los costos aproximados de implementación y dando una idea de la infraestructura TI sobre la cual el diseño de la red planteada puede ser implementada.

1. Marco general del proyecto

1.1 Planteamiento del Problema

En La tecnología Blockchain en su trayectoria hasta la actualidad se encuentra como en los comienzos del internet en los años 90's, pero el conjunto de soluciones que trae consigo esta tecnología es enorme, una de las muchas soluciones que trae para aportar es el cambio del sistema electoral, es decir a la forma en que votamos y elegimos a los mandatarios, todo cambio es bueno y este no es la excepción.

En países como Colombia existe una gran incertidumbre acerca de que "estos comicios sean totalmente transparentes, que no sean manejados por las grandes maquinarias del país y lo más importante que el voto que uno deposite sea tomado en cuenta" (Tapscott & Tapscott, 2017), pero lo realmente importante es que ante tanta incertidumbre exista una forma o manera de que este proceso sea totalmente transparente y en el cual no se puedan modificar los resultados con alguna intención.

El sistema de votación actual es bastante dispendioso porque requiere de una gran logística y despliegue tanto de personas como de gran cantidad de materiales tales como cartón, hojas de papel, lapiceros, tinta, etc. Todos estos materiales son utilizados en gran cantidad y se utiliza para un instante de tiempo corto contribuyendo de tal forma en cierta manera al no cuidado del planeta. La falta de transparencia y vigilancia ha contribuido a que exista una gran abstinencia al votar y no hacer uso de su derecho por parte de las personas, así mismo contribuir a la corrupción del país ya que las elecciones podrían estar siendo manipuladas por algún tipo de maquinaria para alguna conveniencia, silenciando la decisión del pueblo e imponiendo la de las maquinarias y de tal manera siendo un gasto doble porque así las personas voten, la decisión del ganador ya estaría tomada, violando un derecho fundamental de todo un país.

Todo lo anterior, también se produce en gran parte porque el sistema electoral actual lleva funcionando décadas de la misma manera, lo que ha cambiado es el conteo para que sea un poco más ágil y conocer los resultados más rápido. La tecnología Blockchain trae una revolución más que completa ya que basa su funcionamiento en una cadena de bloques que permite a los usuarios generar cualquier tipo de transacción de una forma segura y eliminando todo tipo de intermediarios, así mismo, procesos que se encuentren en el medio de una acción y contribuyendo a que muchos de los problemas del sistema electoral actual que se usa en el país sean solucionados de una forma eficaz, eficiente y segura.

Pregunta Problema: ¿Cómo una tecnología como Blockchain puede aportar al mejoramiento de unas votaciones electorales a nivel nacional, cómo se haría y cuáles serían los aportes de esto a la sociedad?

Responder esta pregunta es importante ya que enfoca toda la energía a desarrollar y realizar un diseño de un prototipo de red Blockchain para un ejercicio electoral a nivel nacional.

Los casos de uso que existen y que se han realizado en el mundo son prototipos, lo cual hace referencia a que son tipos de red Blockchain nuevos aun con variables o procesos por realizar. Para realizar una red de este tipo se debe considerar la escalabilidad de lo que se está proponiendo y pensar en soluciones enfocadas a algunos problemas que aún se tienen como la identificación del votante y la confidencialidad del voto.

Se pretende realizar el diseño del prototipo de una red como esta para Colombia, es decir realizar un prototipo que pueda funcionar en este territorio y que se ajuste o adapte a las normas del sistema electoral a nivel nacional.

1.2 Justificación

El presente trabajo de tesis nace por el motivo de conocer el funcionamiento e interactuar con redes Blockchain. Desarrollando el diseño completo de una red Blockchain para un ejercicio electoral como lo es para este caso, se puede abarcar en un amplio conocimiento en diseño de redes Blockchain con diferentes aplicativos y soluciones que se puedan desarrollar con esta tecnología, buscando el generar valor a usuarios como a las personas, empresas o como lo es para el caso de este proyecto aportando en la mejora de las futuras justas electorales en el país.

Las aplicabilidades de la Blockchain van mucho más allá del Bitcoin, si bien es verdad que la tecnología Blockchain está estrechamente vinculada con todo alrededor de las criptomonedas no es el único uso o aplicabilidad que tiene, el alcance de esta tecnología va mucho más allá, explorando y desarrollando aplicativos en campos como la salud y la política. Un ejemplo puntual, el cual aplica para el desarrollo de este documento es por medio del voto electrónico, y es que “las cadenas de bloques permiten una red en la cual exista un sistema electrónico en el cual las identidades sean protegidas, así mismo haciendo que las votaciones tengan un coste bajo” (Bit2me Academy, 2019).

Blockchain es una tecnología totalmente nueva y en pleno auge con tendencia a que en los próximos años muchas de las cosas que para nosotros son cotidianas se hagan ahora utilizando esta tecnología, tal como una justa electoral. Estos sistemas o redes ya se han implementado en algunos países para realizar elecciones, como el caso de Sierra Leona en el continente de África que

> “se convirtió en el primer país del mundo que uso Blockchain para registrar el 70% del conteo de sus elecciones presidenciales, en las que participaron 16 candidatos, la empresa que desarrolló el aplicativo es Agora, una startup de Blockchain con sede en suiza” (Beamonte, 2018).

Y es que el realizar unas elecciones de cualquier tipo con esta tecnología trae grandes beneficios, uno de ellos es el ahorro de dinero y el cuidado del planeta, debido al ahorro de papel y del despliegue de materiales que se necesitan para unas elecciones, así como reducir la corrupción en el proceso de los comicios, el cual es el beneficio más importante para este caso. Las elecciones con estas redes son totalmente transparentes y se puede realizar el conteo prácticamente que, al instante, mediante un sistema de votación digital el cual usa una cadena de bloques que tendría que ser privada para supervisar los resultados, estamos en frente de una red que permite a los votantes unos comicios justos y transparentes. Blockchain lo puede efectuar básicamente porque descentraliza toda operación o gestión, el control del proceso es ahora de los usuarios, para este caso sería de los supervisores y no de los intermediarios como normalmente sucede.

Existen casos como Venezuela y Brasil que mantienen sistemas electorales electrónicos, que según el documental Hacking Democracy, son bastante vulnerables, junto a la falta de credibilidad en el sistema como a las instituciones públicas que vigilan los comicios, es decir, que lo que demuestra esto es que no es únicamente necesario la automatización de los procesos de votación, “debe existir un sistema el cual garantice la credibilidad y transparencia del proceso electoral, ya que la confianza en el sistema es necesaria” (Preukschat, 2017).

Ahora bien, “La transparencia es pilar fundamental en la tecnología Blockchain ya que está impresa en su ADN” (Rivero, 2018), es por tal razón que el uso de estos sistemas y de redes basados en esta tecnología tan poderosa empiezan a perfilarse como la gran alternativa real a las vulnerabilidades de los sistemas que ya existen hoy en día.

1.3 Objetivos

1.3.1 *Objetivo General*

Realizar propuesta de diseño de un prototipo de red Blockchain para un ejercicio electoral en Colombia, midiendo impactos y beneficios.

1.3.2 *Objetivos Específicos*

1. Analizar los métodos de votación existentes más representativos que permiten el funcionamiento de justas electorales a nivel mundial.
2. Definir los componentes y requerimientos importantes para el funcionamiento de la propuesta de red Blockchain aplicado a este ejercicio electoral.

3. Definir el diseño de la red Blockchain aplicado a este ejercicio electoral a nivel nacional.
4. Evaluar financieramente el despliegue de la red a nivel nacional y viabilidad de la realización de una justa electoral mediante una red Blockchain.
5. Generar recomendaciones y aportes de los beneficios y aplicativos de la implementación de redes Blockchain en el mundo. Especialmente de la implementación de una red Blockchain aplicado a un ejercicio electoral a nivel Colombia.

1.4 Alcance

El alcance que tendrá este proyecto será en base a los objetivos planteados para el desarrollo del mismo. El enfoque principal que tendrá este proyecto de tesis es investigativo y de tipo exploratorio. La razón principal es porque el blockchain es un campo muy nuevo y con actividad mínima acá en Colombia. La realización de este proyecto es con el fin de que con el tiempo se pueda desarrollar e implementar. El desarrollo de este proyecto de tesis está basado en la investigación, recolección de datos y de información, así mismo como el diseño junto con sus beneficios y costo.

Para cada objetivo específico se tendrá un alcance propio de diferente tipo según sea lo requerido en el objetivo con el fin de lograr el alcance en general de todos los objetivos.

Para el desarrollo del proyecto es necesario examinar el tema de una red Blockchain para un ejercicio electoral en Colombia, lo cual es un tema poco estudiado o desarrollado, básicamente un mundo nuevo por descubrir, y es allí donde una investigación Exploratoria nos ayudará a familiarizarnos con esta tecnología y sus términos con el fin de llevar un proyecto investigativo más completo. La meta de este proyecto es describir principalmente esta tecnología sus componentes para su funcionamiento así mismo como describir la situación actual del sistema electoral y los beneficios de la implementación de una red electoral en Blockchain con su correspondiente viabilidad y evaluación financiera, lo cual basándonos en una investigación de tipo Descriptiva que nos permita mostrar los ángulos o dimensiones de cada uno de los aspectos nombrados anteriormente.

En el aspecto general que enmarca toda la investigación del proyecto se hará en base a una investigación Explicativa ya que va dirigida a responder las causas del fenómeno el cual para este caso es la tecnología Blockchain, también nos permite llevar a cabo una investigación y desarrollo de este proyecto de una forma estructurada proporcionando un sentido de entendimiento al resultado de esta tesis.

1.5 Metodología

La metodología que se implementara para el desarrollo de este proyecto de tesis será basada en la estructura que se tiene en los objetivos, está pensada que cumpliendo el primer objetivo sirva para cumplir el segundo y de esta forma hasta cumplir todos los objetivos propuestos.

Como primera parte se empezará definiendo todos los aspectos y componentes que son relevantes para el funcionamiento de una red de Blockchain conociendo las características de la tecnología se podrá comprender un poco mejor el funcionamiento técnico y teórico de una red basada en esta tecnología.

En segunda parte y desarrollando el primer objetivo nos permite ubicarnos en tiempo y espacio de cómo se están llevando a cabo hoy en día las votaciones por medio de tecnología en otros lugares del mundo y cómo se desarrollan acá en Colombia, esto para conocer qué es lo que precisamente se quiere mejorar con esta propuesta.

En tercer lugar, se desarrollará basándose en la información anterior del diseño de la red en Blockchain para un ejercicio electoral a nivel nacional, ya conociendo las características y componentes más importantes y que se deben tener en cuenta, entonces se procederá a realizar el diseño de la gestión del sistema electoral que se propondrá como resultado.

En cuarto lugar, se continuará con el desarrollo de la tesis basándonos en el desarrollo del objetivo anterior, porque conociendo cómo será la gestión, organización y operación del sistema electoral que se plantea, se procede a desarrollar y explicar la parte técnica del funcionamiento del sistema electoral basado en la tecnología blockchain. Los objetivos se separan y se desarrollan en dos, pero uno muy de la mano del otro con el fin de cubrir con el análisis completo del sistema electoral planteado en este trabajo de grado.

En quinto lugar, se realizará la evaluación financiera y factibilidad de este proyecto es decir el costo que tendría esta red y conocer la infraestructura TI sobre la cual se podría implementar el sistema de red blockchain.

Y cerrando se darán unas recomendaciones técnicas, económicas y sociales de la implementación de un sistema electoral basado en blockchain en Colombia.

Básicamente se realizará o implementará una estructura paso a paso para llevar un orden claro y que el tema así mismo como los resultados esperados sean entendibles y notorios.

En la siguiente imagen se observa la metodología planteada y sobre la cual se desarrolla el presente trabajo de grado:

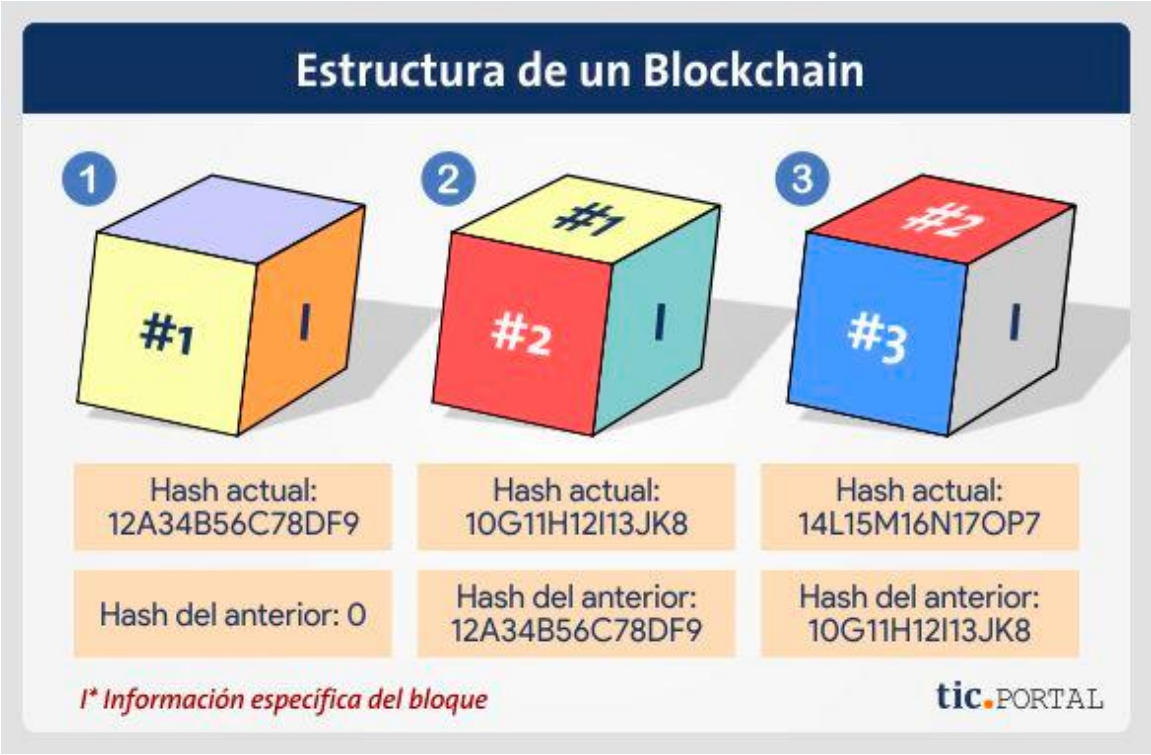
Figura 1. *Imagen Metodología*

Nota. Fuente: el autor.

1.6 Marco Teórico

1.6.1 *Funcionamiento Básico de Blockchain*

Figura 2. *Estructura Blockchain*



Nota. Adaptado de Blockchain (cadena de bloques) [figura], por Tic Portal, 2018. https://www.ticportal.es/glosario-tic/blockchain/

Del gráfico anterior, figura 1, se puede obtener una idea de la estructura y términos importantes de la cadena de bloques.

A continuación, se hará referencia específicamente al funcionamiento y se enfatizará en los componentes más importantes de un bloque y con la ayuda de la figura 1 se busca que se refuerce su explicación y entendimiento.

Entonces, Blockchain es una base de datos, la cual va registrando valores y transacciones; el propósito de esta tecnología es mucho más que simplemente ser una base de datos gigante, puesto que esta base de datos es distribuida y permite la transferencia de información que además se realiza de forma cifrada.

La gran debilidad de un sistema informático es que es hackeable, pero entonces ¿cómo evita esto Blockchain? Lo evita no con un súper poderoso antivirus, ni con un vigoroso firewall. “Blockchain se auto protege gracias a su propia estructura o arquitectura, como su nombre lo indica es una cadena de bloques y cada bloque puede

contener diferentes tipos de información" (Porxas & Conejero, 2018). Así pues, los bloques se conforman de tres cosas principales e indispensables:

La primera: la información, por ejemplo, en el caso de bitcoin contiene la información relacionada con la transacción, es decir, emisor, receptor, cantidad, etc.

La segunda: el Hash, el cual es muy importante, ya que es el número de identificación del bloque. Se trata de un número único e irrepetible. Cada uno de los bloques tiene su propio hash. Este se crea basándose en la información que se encuentra en el bloque, es por esta razón que existe únicamente uno.

La tercera: contiene el hash del bloque anterior, por lo que cada bloque queda conectado con su predecesor y su sucesor, es por tal razón que es una cadena de bloques.

Ahora bien, conociendo de lo que se compone un bloque se puede entender "la razón de que no sea hackeable, una razón es el hash" (Porxas & Conejero, 2018), y es que como se mencionaba anteriormente, este número es inalterable y dicho número se crea basándose en la información propia del bloque, eso significa que, "si cambia el contenido o información del bloque, automáticamente cambia el hash" (Porxas & Conejero, 2018), básicamente es como si el bloque cambiará de forma, y al cambiar de forma dejará de encajar, por lo tanto, la cadena quedaría invalidada.

La otra razón está basada en el funcionamiento de la red, ya que muchos nodos están observando el comportamiento de la red todo el tiempo. Y no es que exista una única base de datos, cada usuario de Blockchain tiene una 'copia' de ella, es decir, contiene una copia idéntica y completa de la red Blockchain. El contenido de las transacciones está bloqueado, referente a fechas, tiempos, participantes y volúmenes de cada transacción. Dado que muchos nodos están observando todo el tiempo, "si un usuario altera la información de su copia, la comunidad de la red se daría cuenta y por ende 'su' versión de la base de datos es anulada y queda sin efecto" (Porxas & Conejero, 2018). Esta es la gran diferencia: la seguridad y la certificación de los documentos en Blockchain la dan los mismos usuarios, no un intermediario.

Los usuarios son los mismos quienes gestionan la red, "las redes blockchain tienen dos motivos principales por los cuales capta usuarios: uno es simplemente para usar el sistema y el otro es crear nuevos 'blocks' para la 'chain'" (Porxas & Conejero, 2018). Los encargados de realizar esto último son los mineros que son los mismos nodos, muchos de los usuarios de la red no están allí para únicamente usar los servicios de la red, están allí para crear nuevos bloques. A medida que se van firmando contratos o haciendo transferencias o para lo que se esté utilizando la red, existe la necesidad de almacenar esa información en un nuevo bloque.

Para añadir un nuevo bloque se debe resolver un problema u operación matemática de altísima complejidad, para resolverlo se necesita una gran potencia de computación, de esta forma “los mineros ponen su capacidad de procesamiento a tope para intentar resolverlo” (Porxas & Conejero, 2018). Una vez el minero crea haberlo resuelto, el resto de la comunidad verifica que la solución es la correcta. Si es correcta, el nuevo bloque se añade a la cadena, la información queda consolidada y la transacción se ejecuta. El minero que encuentra la clave obtiene una recompensa o pago, para el caso de bitcoin es de “12,5 bitcoins, y cada bitcoin tiene un valor aproximado a los 10.500 dólares” (Porxas & Conejero, 2018).

Blockchain es una tecnología P2P (Peer to Peer) lo que significa que es únicamente entre dos puntos, pero que toda la red puede ver y tiene una copia de tal transacción, eliminando así a los intermediarios y cualquier posibilidad de alteración o penetración a la red, o simplemente que la misma sea hackeada, pues se requeriría tener un control sobre todos los registros que existen en la red y “necesitaría modificar o alterar la transacción en más del 70% de la red al mismo tiempo” (Limanorum, 2018), lo que hace que no sea posible modificar algo en la red sin que todos los nodos o participantes se den cuenta, haciéndola muy segura.

El Blockchain cuenta con unas características principales, basado en la información administrada por Limanorum (2018) y consecuentemente se analizarán, las cuales se definirán a continuación.

Cifrado: Su función principal es la criptografía de los datos, lo que se traduce a que únicamente el remitente y el destinatario conocen todo el contenido de la transacción.

Cronología de operaciones en bloques: Todas las transacciones de la red se van almacenando en bloques y estos a su vez se guardan de forma cronológica.

Inalterabilidad: La seguridad de esta tecnología es bastante alta ya que la información no se puede borrar ni modificar, dada su distribución, por lo que se puede consultar en cualquier momento.

Confiable: La tecnología funciona a través de “un protocolo de consenso que permite que se incluya información confiable sin que se tenga que establecer confianza entre los nodos” (Limanorum, 2018), es decir, que la información de la transacción debe ser la correcta y la verídica porque de lo contrario la información que no cumple con el estándar de la red, inmediatamente la misma red lo repele y no deja realizar la transacción.

Transparencia: Los usuarios de la red pueden en cualquier momento ingresar y verificar o buscar los registros generados de las transacciones en cualquier momento.

1.6.2 *Tipos de Blockchain.*

Existen tres tipos de Blockchain:

1.6.2.1 *Blockchain Pública*

Es en la que puede acceder cualquier tipo de usuario y que no tiene ninguna restricción, solo se necesita una computadora con buena capacidad de procesamiento y acceso a internet, es válido resaltar que “los usuarios en este tipo de blockchain interactúan de forma privada” (Preukschat, 2017).

1.6.2.2 *Blockchain Privada*

A diferencia de la pública, a esta únicamente se puede entrar con permiso o autorización de la red; así, “el mantenimiento y funcionamiento dependen de una sola organización la cual guarda los registros y no siendo públicos” (Preukschat, 2017).

1.6.2.3 *Blockchain Híbrida*

Es una síntesis de las anteriores, “ya que mientras el acceso es restringido, los registros son descentralizados” (Preukschat, 2017), pero pertenecientes a una sola organización que es la misma que autoriza los contenidos que sean visibles.

1.6.2.4 *Blockchain en Colombia.*

En Latinoamérica el blockchain ha venido creciendo a paso lento pero seguro, y “se espera que alcance US$1.356 millones para 2024” (Semana.com, 2019). Argentina y México son los países con mayores avances. En Colombia, su uso aún es incipiente. “Las proyecciones apuntan a que este negocio pasará de US$4,8 millones registrados en 2018 a US$92,7 millones en 2024” (Semana.com, 2019), según datos de la consultora Frost & Sullivan y cálculos de la vicepresidencia de Innovación e Inteligencia Sectorial de Procolombia.

> “El experto dice que en Colombia se ha avanzado mucho en cuanto a la usabilidad, pero no en el desarrollo. Sin embargo, destaca lo hecho por Ruta N, en Medellín. Recientemente allí se inauguró el Centro para la Cuarta Revolución Industrial, que tiene al Blockchain como una de las tecnologías priorizadas para investigación, desarrollo y aplicación” (Semana.com, 2019).

Esta tecnología brinda transparencia y confianza. Los empresarios coinciden en que las empresas no han entendido muy bien el Blockchain debido a la falta de conocimiento. El papel de la academia es clave para que este negocio se desarrolle y el país logre ampliar la oferta más allá de los *commodities* y los productos tradicionales.

1.6.3 *Topología de red.*

La tecnología Blockchain se presenta como capaz de dar un giro a este sistema, puesto que, mediante un protocolo informático de código abierto, permite la llevanza de bases de datos de forma descentralizada, «distribuida», sin necesidad, así, de contar

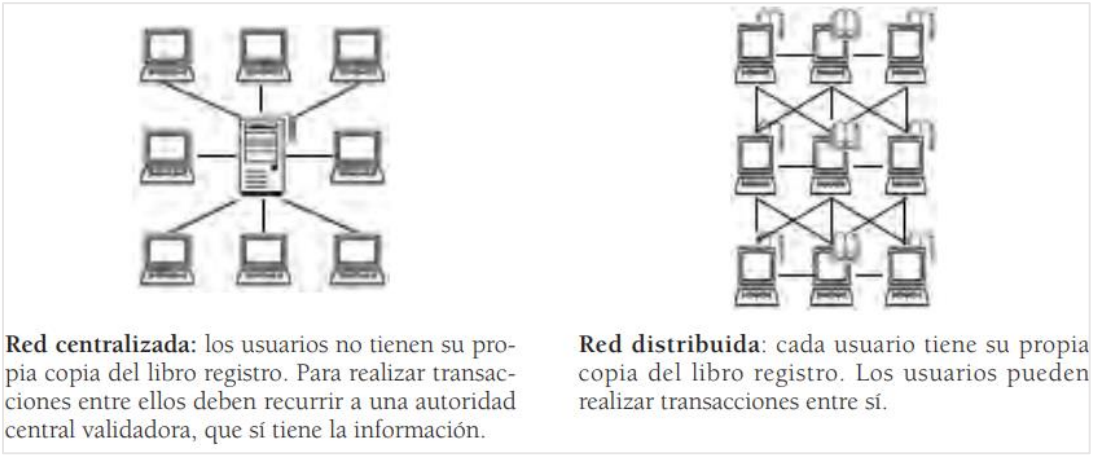
siempre y en todo caso con una «autoridad central», o entidad poseedora de la información, que actúe como garante de su corrección y como intermediaria en las transacciones realizadas sobre su base.

La tecnología Blockchain, como distributed ledger technology o DLT (tecnología de red o registro distribuido) que es, permite crear redes para compartir libros registro de transacciones electrónicas, muy similares a los libros de contabilidad o, dicho de otro modo, bases de datos digitales compartidas. Su singularidad reside en el hecho de que estos libros están distribuidos entre los participantes de la red, quienes se encargan —todos ellos— de su llevanza. En este tipo de redes, cada uno de los nodos o usuarios (ordenadores) tiene una copia original del libro registro y, por lo tanto, cada uno de ellos es capaz de determinar si las operaciones planteadas por el resto de los usuarios de la red pueden realizarse o no. La llevanza de libros registro distribuidos la realizan, en consecuencia, los propios usuarios de la red blockchain sobre la que se ha desarrollado la concreta base de datos en cuestión.

Este hecho significa que todas las transacciones que se realizan en tal red son aprobadas y validadas por los propios nodos, que son capaces de verificarlas y validarlas mediante cotejo con su propia copia del libro registro. Tal aprobación se lleva a cabo por consenso, de modo que “cuando la mayoría de los nodos está de acuerdo con una actualización del libro registro (i.e., la incorporación de nuevas transacciones), el contenido aprobado queda incorporado por la propia decisión del grupo, sin necesidad de intervención de entidad validadora o certificadora de la información”. (Defelipe, 2018)

En la siguiente imagen, figura 3, se puede observar la topología para una red centralizada la cual es como se utilizan la mayoría de redes actualmente en comparación con a una red descentralizada, que es cómo funciona el blockchain; este tipo de topología es la que se utilizara para el diseño de la red a nivel nacional.

Figura 3. *Tipos de redes: Centralizada Vs. Descentralizada*



Nota. Fuente: el autor.

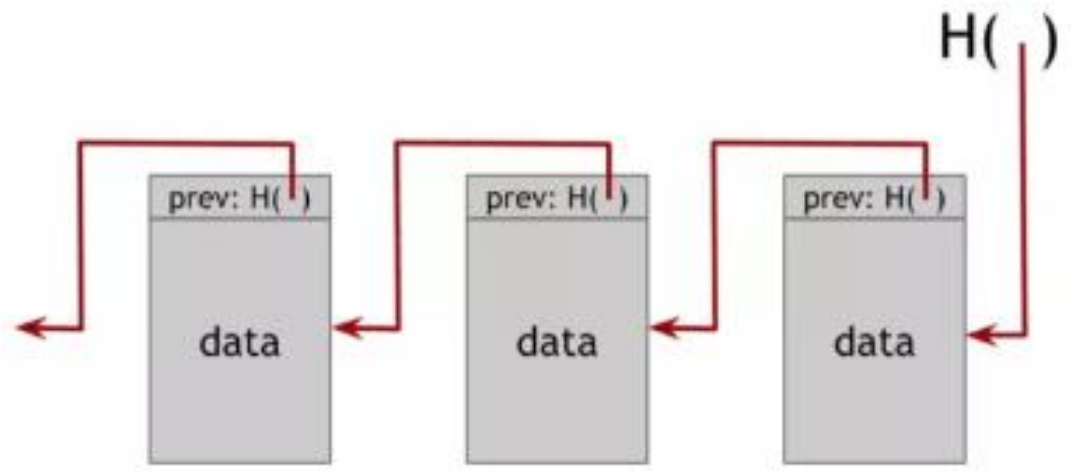
1.6.4 *Estructura de una cadena de bloques.*

Los bloques de información se enlazan mediante apuntadores hash que conectan el bloque actual con el anterior y así sucesivamente hasta llegar al *bloque génesis*.

La cadena de bloques es almacenada por todos aquellos nodos de la red que se mantienen en sincronía con ésta.

En la figura 4 se puede observar como es la estructura de una cadena de bloques, como se conforma y como se unen los bloques con las transacciones entre si.

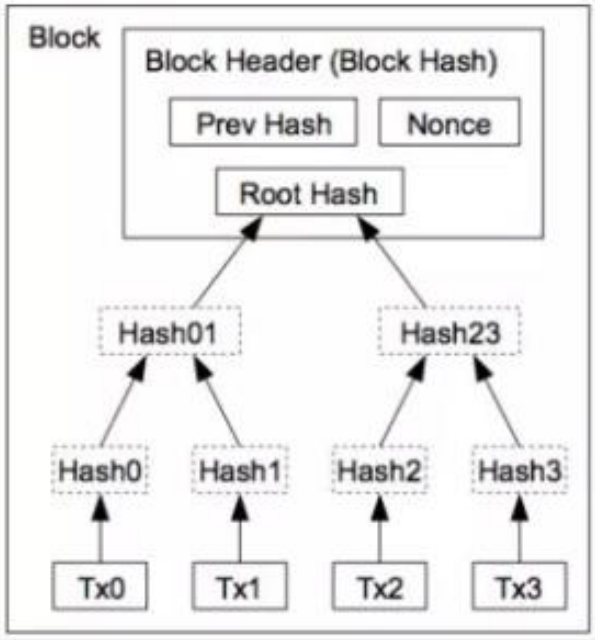
Figura 4. *Estructura de una cadena de bloques.*



Nota. Adaptado de *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (libro). [Figura], por Narayanan et al. Universidad de Princeton, 2016, https://books.google.com.co/books?hl=es&lr=&id=LchFDAAAQBAJ&oi=fnd&pg=PP1&dq=Bitcoin+and+Cryptocurrency+Technologies+universidad+princeton&ots=AsnM9X3JlI&sig=G5cOTau2ZiJEfX9tVASUbW1tSq0

Cada bloque perteneciente a la cadena de bloques contiene información referente a “las transacciones relativas a un periodo (agrupadas en una estructura denominada Merkle Tree), la dirección criptográfica (apuntador hash) del bloque anterior y un número arbitrario único (nonce)” (Bit2me Academy, 2019).

Figura 5. *Estructura Hash*



Nota. Estructura e información contenida en un bloque de la cadena de bloques (block chain). Adaptado de *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Figura]. Por Nacakamoto S., (N.F.). https://bitcoin.org/bitcoin.pdf

Cómo se incorpora la información al libro registro distribuido: la cadena de bloques En el libro registro, todas y cada una de las transacciones se agrupan en bloques, que no son más que «paquetes» con la información sobre las últimas transacciones realizadas en un determinado periodo de tiempo. Estos bloques se van añadiendo de forma sucesiva al libro registro en la red a medida que se van formando. Cuando un bloque de información se incorpora al libro registro, queda irreversiblemente vinculado al bloque aprobado anteriormente, de modo que se encadenan entre ellos, y de ahí que esta tecnología se denomina “cadena de bloques».

Esta vinculación entre los bloques es posible gracias a un robusto sistema criptográfico, que convierte las redes blockchain en registros prácticamente inalterables. El ejercicio de validar las transacciones, la creación de los bloques y su posterior incorporación al registro distribuido es realizado por los llamados nodos validadores.

Estos usuarios de la red cotejan su versión del libro registro con las transacciones constantemente propuestas por los usuarios para verificar que:

(i) el usuario emisor y el receptor tienen cuentas que existen y

(ii) el emisor tiene disponible aquello que quiere transferir o mover.

Si el contenido de la transacción es coherente con la copia del libro registró distribuido del nodo validador, este la incluirá en un bloque. “Una vez que el bloque se

«llena» de transacciones propuestas, el nodo validador lo someterá a la aprobación del resto de los nodos validadores" (Beamonte, 2018), que lo aprobarán si, nuevamente, el contenido coincide con su respectiva versión del registro. Si la mayoría de los usuarios no acepta el contenido, esta parte del bloque no será incorporada al registro.

Ahora bien, una vez que un bloque se añade al registro, no puede eliminarse de ningún modo: "mientras que destruir o corromper un registro tradicional requiere un ataque al intermediario" (Beamonte, 2018). Un sistema blockchain requiere un ataque simultáneo a un porcentaje significativo de copias del libro registro, que, por encontrarse físicamente almacenadas en el ordenador de cada usuario, son de muy compleja alteración en la mayoría de redes.

1.6.5 *Elementos fundamentales en una red Blockchain.*

La cadena de bloques es un registro de todas las transacciones que tienen lugar "empaquetadas" en bloques que los mineros se encargan de verificar.

Posteriormente serán incluidas en la cadena una vez validadas y distribuidas a todos los nodos que forman la red, teniendo en cuenta que, "actualmente, la cadena de bloques ocupa unas 40 gigas" (Blockchain.com, 2021)

Veamos cada uno de estos elementos en detalle:

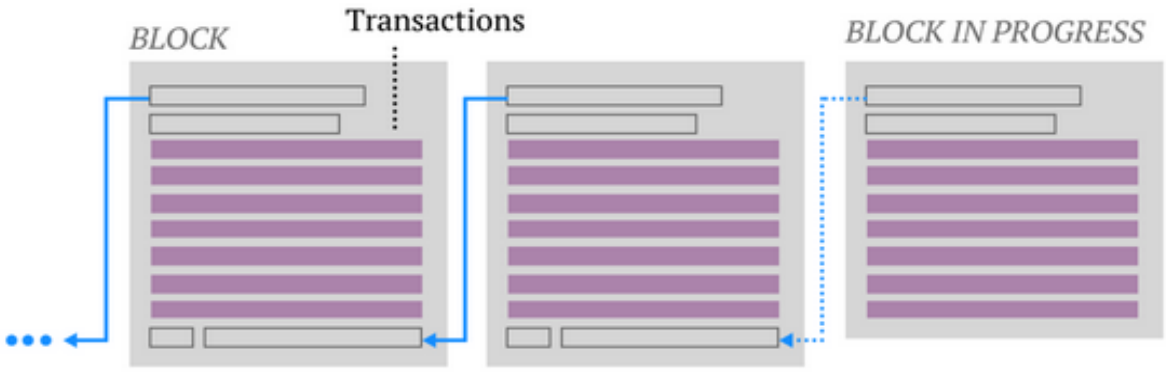
1.6.5.1 *Bloques:*

Un bloque es un conjunto de transacciones confirmadas e información adicional que se ha incluido en la cadena de bloques.

Cada bloque que forma parte de la cadena (excepto el bloque generatriz, que inicia la cadena) está formado por:

1. Un código alfanumérico que enlaza con el bloque anterior
2. El "paquete" de transacciones que incluye (cuyo número viene determinado por diferentes factores)
3. Otro código alfanumérico que enlaza con el siguiente bloque.

Figura 6. *Bloques para una transacción.*



Nota. Fuente: el autor.

El bloque en progreso lo que intenta es averiguar con cálculos el tercer punto anteriormente indicado. Un código que sigue unas determinadas reglas para ser válido y sólo puede sacarse probando sin parar.

1.6.5.2 *Mineros:*

Los mineros son ordenadores/chips dedicados que aportan poder computacional a la red de bitcoin para verificar las transacciones que se llevan a cabo.

Cada vez que alguien completa un bloque recibe una recompensa en forma de bitcoins (actualmente 25) y/o por cada transacción que se realiza.

Si pensamos en la minería del oro, “esta consiste en remover tierra con pesadas máquinas para obtener oro en cantidad suficiente para pagar los costes de explotación y obtener beneficio” (Criptonoticias, 2021). Lo mismo pasa en la minería de bitcoin, con la salvedad de que “la maquinaria son equipos informáticos complejos que realizan cálculos computacionales” (Bit2me, 2021) y como compensación obtienen dos incentivos:

- Nuevos bitcoins que se ponen en circulación
- Las comisiones de las transacciones

“Los mineros reciben un nuevo problema matemático cada diez minutos y el más rápido en resolverlo se lleva las nuevas monedas que se ponen en circulación” (Rivero, 2018). Este problema matemático se basa en cálculos aleatorios que tienen como objetivo encontrar la solución y así obtener la validación del bloque. “Quien descifra esto se llevará la recompensa, siempre y cuando el resto de miembros de la red diga que la respuesta es correcta” (Rivero, 2018).

1.6.5.3 Nonce:

En criptografía, el término *nonce* es usado para referirse a un valor que solamente puede ser usado una vez. “Este número único o nonce, es un número aleatorio emitido por los mineros a través de la Prueba de Trabajo (PoW)” (Criptonoticias, 2021), que sirve para autenticar el bloque actual y evitar que la información sea reutilizada o cambiada sin realizar todo el trabajo nuevamente.

1.6.5.4 *Nodos:*

Un nodo es un ordenador/chip conectado a la red bitcoin utilizando un “software que almacena y distribuye una copia actualizada en tiempo real de la cadena de bloques” (Bitcoin, 2021).

Cada vez que un bloque se confirma y se añade a la cadena se comunica a todos los nodos y este se añade a la copia que cada uno almacena.

Una de las mayores curiosidades que tiene el protocolo bitcoin es que “cada unidad no es un archivo como tal que se envía como si fuese una película o canción, al estilo de un protocolo P2P como puede ser BitTorrent” (BBVA, 2017).

En realidad, lo que se produce es un registro del cambio de propiedad de una cantidad determinada de bitcoins en la cadena de bloques.

1.6.6 *Protocolo P2P (peer to peer)*

“Para el 2008 el sistema financiero global se fue al piso” (BBVA, 2017). Puede que aprovechando este momento o situación que se vivía en ese momento, una persona o algunas personas con el pseudónimo de Satoshi Nakamoto, revelaron el protocolo de un nuevo sistema de pago electrónico directo y entre iguales, el famoso Peer-to-Peer o P2P, el cual usaba una criptomoneda llamada Bitcoin, teniendo en cuenta que la diferencia de una criptomoneda (monedas digitales) y una moneda tradicional se basa en que las criptomonedas no las crean ni las controlan los países.

El P2P estableció una serie de normas en forma de computación distribuida, las cuales garantizaban la integridad de la información intercambiada entre esos miles de millones de ordenadores sin la necesidad de pasar o que exista un tercero.

Esta forma de funcionamiento fue realmente cautivante para las personas que les gusta o que trabajan con computación, y no tardó mucho tiempo para que esto llegara a casi todas las partes del mundo, empezando por los gobiernos hasta modelos de negocios existentes hoy en día.

Este protocolo es el fundamento de un creciente número de registros globalmente distribuidos llamados cadenas de bloques (Blockchain), el más grande de los cuales es bitcoin. Las cadenas de bloques permiten enviar dinero de manera directa y segura de

una persona a otra sin pasar a un banco o algún intermediario. A gran diferencia del internet que es más una gran red de información, el blockchain es un internet o red del valor o del dinero, también es una plataforma que permite a todo el mundo saber lo que es verdad hablando claramente de información que se registre de una forma estructurada.

Definiéndolo de una forma básica Blockchain es un código fuente el cual es libre, es decir todo, el mundo o el que desee puede descargarlo gratuitamente, ejecutarlo y usarlo con el fin de desarrollar nuevas herramientas de gestión de transacciones en línea, como tal esta tecnología aporta la posibilidad de crear infinidad de aplicaciones nuevas y de cambiar de igual forma infinidad de cosas.

Usa una encriptación que incluye claves públicas y privadas lo cual garantiza una total seguridad. Con esta tecnología ya no se tendría que estar preocupados porque funcionen de forma correcta los firewalls o que exista una persona que sea corrupta o ladrona.

Cada diez minutos asemejándose a un ritmo cardíaco de una red de bitcoin, todas las transacciones realizadas se comprueban, ordenan y almacenan en un bloque que se une al bloque anterior, creándose así una cadena. Cada bloque debe referirse al bloque anterior para ser válido. Esta estructura registra exactamente el momento de las transacciones y las almacena, evitando que nadie pueda alterar el registro. En caso de que alguien quiera robar un bitcoin, tiene que reescribir toda la cadena de bloques a la vista de todos, lo que sería prácticamente imposible.

1.6.7 *Características de Blockchain.*

Existen tres características de la blockchain que son las importantes o relevantes que sirven para comprender el funcionamiento. A continuación, veremos cada una de ellas.

1.6.7.1 *Transparencia.*

Ya teniendo muy en claro que todos los usuarios de las redes blockchain tienen acceso al libro de registro, lo cual implica que todos los usuarios de la red tienen la información sobre las transacciones que se efectúan por el grupo. En algunas redes como por ejemplo en la de Bitcoin o Ethereum los usuarios que no forman parte de la red también pueden el contenido de la cadena de bloques, a lo cual se agrega que se trata de protocolos informáticos de código abierto, por lo que el acceso al diseño de la programación es de igual forma libre.

Pero se debe tener algo claro para que no existan confusiones, al decir o hacer referencia a que una de las características es la transparencia no significa que podamos conocer el autor de las transacciones en todos los casos.

1.6.7.2 *Irrevocabilidad.*

Después de que la información ya se encuentre en una blockchain, no es posible eliminarla de ahí, salvo algunas pocas excepciones. Básicamente en otras palabras la información es poseída por todos los usuarios, por lo que es imposible eliminarla de la red. Los datos incorporados a la cadena de bloques se distribuyen a todos y cada uno de los nodos que intervienen en la red.

1.6.7.3 *Inmutabilidad.*

Gracias a la consecuencia del encadenamiento sucesivo de los bloques basado en la criptografía que son los famosos hashes, el contenido de la cadena de bloques es inmutable.

Si un nodo decide cambiar el contenido de la cadena de bloques alterando una transacción, provocará que el contenido de su versión del libro registro varíe, haciendo que este cambio sea fácilmente identificable por el resto de los nodos. Por lo tanto, al momento de someter a aprobación una nueva transacción, estos no aceptaron su versión del registro, ya que el contenido es diferente a la inicial.

2. Analizar los Métodos de Votación Existentes Más Representativos que Permiten el Funcionamiento de Justas Electorales a Nivel Mundial.

A nivel mundial se tienen diferentes modelos de votación por los cuales sus habitantes eligen a sus mandatarios, dentro de todos estos existen modelos muy antiguos, los cuales se llevan usando desde hace muchos años y sobre los cuales se tienen dudas de su veracidad al 100%. También existen métodos mejorados o con apoyo de la tecnología como el voto electrónico el cual aporta una mejora, pero igual con algunos vacíos y por ultimo están los modelos más actuales que proponen algo totalmente diferente a lo ya existente.

A continuación, realizaremos un análisis de cada uno de los métodos más utilizados a nivel mundial tal como el método de voto tradicional, es decir con papeletas o tarjetones y urnas, también el método de voto electrónico el cual es usado actualmente en varios países y por último el método de votación con tecnología Blockchain.

2.1 MÉTODO DE VOTO TRADICIONAL

Esta es quizás la forma de voto más antigua y utilizada por gran parte del mundo, parte de un principio muy importante y es el de resguardar la democracia. A lo largo de mucho tiempo para elegir un mandatario las votaciones se desarrollan de la forma tradicional y más conocida que es la de acercarse a la casa electoral y realizar su derecho al voto de forma física en un papel.

Se analizará y explicará específicamente como funciona este método tradicional en Colombia.

Inicialmente la persona que ejercerá su derecho al voto debe acercarse al lugar habilitado para votar y en donde se realizó el registro previo, este lugar es el sitio de votación el cual lo determina la registraduría para que funcionen las mesas de votación. Detrás de todo esto se encontrará todo un sistema con el fin de garantizar que el voto no sea manipulado, sea transparente y legal. La persona debe solicitar a la mesa de votación que es el sitio habilitado por la registraduría donde el ciudadano debe votar, el tarjetón o tarjeta electoral que es el documento en el cual el sufragante, en ejercicio del derecho al voto, marca su preferencia electoral, el sufragante se dirige a la urna, ejerce su derecho, y luego se acerca a la urna y lo deposita, esta es la parte que desempeña el usuario o rol que juega dentro del sistema.

Técnicamente el usuario pierde el rastro total de su voto y deposita toda su confianza en el sistema con el fin de que el voto sea contabilizado. La mesa de votación está compuesta por personas seleccionadas por la Registraduría Nacional para que cumplan la función de jurados de votación los cuales son ciudadanos seleccionados

mediante sorteo, para atender la mesa de votación, hacer los escrutinios correspondientes y entregar los resultados de las votaciones en los documentos electorales correspondientes.

Externamente están los testigos electorales, el cual es un ciudadano designado por un candidato o una colectividad política para vigilar las votaciones y presentar reclamaciones ante los jurados de votación en los escrutinios de mesa, también cumplen la función de juez, pero no hacen parte de las mesas de votaciones, sino que son los jueces de que el proceso realizado por la mesa de votaciones se realice de forma transparente.

Al finalizar las votaciones la mesa de votaciones abre la urna y realiza el conteo de votos y los documenta, en un formato que se llama Cuenta votos el cual corresponde a un formulario que se suministra a los jurados de votación para facilitar la contabilización (conteo) de los votos por cada candidato.

Consta de unas filas que poseen el nombre de candidatos y otras columnas donde se va registrando el voto obtenido por cada uno de los aspirantes, este proceso hace parte del Escrutinio, en donde participan los jurados de votación, las comisiones escrutadoras y el Consejo Nacional Electoral, para proceder al cómputo de los sufragios, resolver las cuestiones de hecho y de derecho que se aleguen con fundamento en las causales legales de reclamación y hacer las declaratorias de elección a que hubiere lugar, básicamente es la función pública mediante la cual se verifican y consolidan los resultados de las votaciones.

Es un método el cual tiene interacción con muchas personas y el correcto funcionamiento de este método depende en gran medida de la correcta labor que las personas que interactúan realicen, “en este método el uso de la tecnología es limitado, su mayor uso es para el almacenamiento de la data” (Registraduría Nacional del Estado Civil, 2021).

En la siguiente imagen se puede observar un pequeño panorama para tener una idea algo más clara de cómo es el funcionamiento para unas votaciones que se desarrollen de forma tradicional en especial en Colombia.

Figura 7. *Votaciones en Colombia*

Nota. Puesto de votación de elecciones presidenciales 2018 en Colombia. Adaptado de *Países andinos acuerdan lucha conjunta contra desinformación en época electoral* (Artículo web), 2021, [Fotografía], https://www.dw.com/es/pa%C3%ADses-andinos-acuerdan-lucha-conjunta-contra-desinformaci%C3%B3n-en-%C3%A9poca-electoral/a-58900151

2.1.1 *Ventajas y desventajas del método tradicional*

En el análisis que se está desarrollando del método tradicional del voto se traerá a colación las ventajas y desventajas que este presenta con el fin de tener un punto de comparación con los demás métodos de votación.

2.1.1.1 *Ventajas*

Las ventajas del método tradicional de voto son:

- Una de las ventajas es la experiencia del usuario, es decir, cuando el votante deposita su voto en la urna experimenta una sensación de confianza en que su voto está seguro y será contabilizado.
- Las personas mayores o las personas que necesiten ayuda en el proceso de votación, pueden obtener la ayuda y entendimiento más fácil y ejercer su derecho al voto.
- Todas las personas que se puedan desplazar al lugar de votación lo podrán hacer, lo que se busca resaltar en este caso que en Colombia no todos tienen acceso a la tecnología, entonces al poder desplazarse a la sede de votación podrá ejercer su derecho al voto.

2.1.1.2 *Desventajas*

- Los altos costos de las votaciones de forma tradicional exceden por mucho cualquier otro método me votación.

- ❖ Se pierde la trazabilidad del voto, se depende de la confianza que el votante deposite en el sistema de voto tradicional.

2.2 Método de Voto Electrónico

Para cualquier método de votación el voto debe ser legítimo y para esto debe cumplir con ciertas condiciones básicas de seguridad. El voto debe ser: secreto, universal y único. El voto electrónico no es la excepción y está concebido de tal forma que cumpla con los requisitos básicos.

El voto electrónico para su funcionamiento hace uso de mucha tecnología y se asemeja al método tradicional en cuanto al proceso. Es importante tener en claro que los sistemas de voto electrónico no son en realidad una novedad, hace años que se tratan de poner en marcha sistemas que resuelvan un problema tecnológico que es mucho más importante de lo que uno podría creer. Las implementaciones son variadas y los grados de automatización en cada una de ellas es muy distinto.

2.2.1 *Casos de Éxito*

Como ya se había nombrado anteriormente el método de voto electrónico lleva implantado muchos años y funciona actualmente en muchos países. Brasil, India, Venezuela o los Estados Unidos son los países que a nivel mundial han estado más interesados en implantar el i-voting que es como se conoce comúnmente al voto electrónico.

Brasil es uno de los países que más resalta en el uso del voto electrónico, “desde 1996 que fue cuando se evaluaron y desde ese momento se empezaron se han ido utilizando en varios y diferentes procesos electorales” (Euskadi.eus, 2021). Uno de los ejemplos más valiosos en donde se utilizó y a la mayor escala fue para las elecciones presidenciales de 2010, en estas elecciones “intervinieron 135 millones de votantes y en las que el resultado se conoció en una hora y quince minutos después de que los colegios electorales cerraran las puertas” (Pastor, 2016). La aceptación del sistema es notable, tanto que por ejemplo Brasil presta sus máquinas en forma de alquiler a países como Paraguay o Ecuador, en donde también se han realizado procesos electorales con la tecnología del voto electrónico.

2.2.2 *Países con sistemas de voto electrónico implantados en el mundo.*

El método de voto electrónico lleva implantado en algunos países del mundo durante un largo tiempo, demostrando gran adaptabilidad, funcionamiento y aceptación por parte de los votantes. Esto demuestra que como todo sistema no es exactamente un 100% y tiene falencias, pero así mismo demuestra que tiene ventajas valiosas ante el sistema tradicional y por tal razón a nivel mundial algunos países lo utilizan, estos son:

En Europa los países que tienen un sistema de voto electrónico implantado son:

- Bélgica: Es uno de los países que a nivel mundial tiene un método de voto electrónico más avanzado, puede ser por el tiempo que lleva usando este método el cual se implementó “desde 1989, allí se empezó utilizando unas tarjetas de banda magnética en donde por medio de una pantalla donde los votantes realizaban su elección” (Euskadi.eus, 2021), esta información se guardaba en las tarjetas y estas posteriormente se depositaban en una urna que leía y computaba la información.

> “Para 2010 comenzó un proceso de licitación para la selección de un nuevo sistema o actualización del ya existente, el sistema nuevo se basa en una urna electrónica con pantalla táctil y con posibilidad de imprimir un comprobante del voto en papel para la auditoria del resultado” (Euskadi.eus, 2021).

Una de las últimas actualizaciones en las que se ha avanzado notablemente es la trazabilidad del voto, para las elecciones del 25 de mayo de 2019 en los puestos de votación de voto electrónico, el votante tiene la certeza de trazabilidad de su voto, porque “al momento de sufragar la maquina imprime una papeleta encriptada, sobre la cual puede confirmar y validar a través de un lector antes de depositarla en una urna” (Euskadi.eus, 2021).

- Estonia: En este país “su primer paso en el método de voto electrónico fue para el 2005” (Euskadi.eus, 2021) y es el primer país en donde fue posible votar a través de internet, mostrando una posibilidad que se tiene contemplada también en otros países que votan de forma electrónica pero de la cual nadie tomaba los riesgos, “en 2011 el 25% de los votantes lo hicieron a través de internet” (Euskadi.eus, 2021), otra de las novedades que tiene en particular el método de voto electrónico en Estonia es que los votantes pueden votar hasta seis días antes del día de las elecciones y lo pueden hacer de varias formas y el voto que será tenido en cuenta para el conteo será el último. Actualmente y tras varias actualizaciones a su método de votación para las elecciones parlamentarias de 2019 “ejerció voto un 44% mediante el sistema de voto electrónico, demostrando la gran acogida y confianza de votar de esta forma en ese país” (Euskadi.eus, 2021). Para realizar su voto electrónicamente la ciudadanía tiene que haberse registrado anteriormente como votante, contar con un computador con conexión a internet, documento nacional de identidad.

- Bulgaria: En este país se realizaron las elecciones al parlamento para el 2021 con máquinas electrónicas, excepto en colegios con menos de 300 votantes registrados, hospitales y otras instituciones sociales, se presentaron fallas técnicas por su reciente implantación de este sistema, y por tal razón, “se tuvo que

suspender el uso de dichas máquinas y utilizar papeletas como el método tradicional para 56 colegios electorales de los más de 12 mil" (Euskadi.eus, 2021).

En América los países que tienen un sistema de voto electrónico implantado son:

- Brasil: El uso del voto electrónico en el país se empezó a implementar "para el año 1995 para cuando se aprobó la Ley Electoral e iniciando su implantación en 1996 con urnas electrónicas" (Euskadi.eus, 2021). En América, Brasil ha avanzado rápidamente en estandarizar este tipo de método de votación; tanto así que, "para el año 2002, el 100% de los votos presenciales fueron emitidos electrónicamente y para las elecciones generales de 2010 aproximadamente cuatro millones de electores usaron urnas biométricas" (Euskadi.eus, 2021), siendo un proceso que se ha ido generalizando en las elecciones.

  "En las elecciones presidenciales de octubre de 2014 más de 23 millones de ciudadanos utilizaron la urna biométrica" (Euskadi.eus, 2021), demostrando lo anteriormente expuesto. Desde allí todas las votaciones que se realizan en Brasil son con el uso de la tecnología del voto electrónico siendo uno de los países con mayor adaptabilidad y uso de este método. "En las ultimas elecciones del 2018 también se usó pero con la novedad de que la impresión del voto no se realizara ya que no cumplía con uno de los principios y es el secreto del voto" (Euskadi.eus, 2021), algo para resaltar es que Brasil presta sus máquinas a modo de alquiler a otros países para realizar sus procesos electorales.

- Estados Unidos: Uno de los países con la trayectoria más larga en cuanto método de voto electrónico o de "la automatización del proceso de votación es quizás Estados Unidos, desde 1892 en donde debuto la primera máquina de votación llamada *Myers Automatic Booth*" (Euskadi.eus, 2021). Esta máquina se trataba de un sistema basado en el uso de palancas mecánicas, en el que a cada candidato se le asignaba una palanca.

  "En 1930 estas máquinas fueron instaladas en las principales ciudades del país y para 1960 casi la mitad de la población hacia uso de estas para votar" (Euskadi.eus, 2021). En Estados Unidos no existe únicamente un sistema de votación, "para 1980 ya existían cinco tipos de sistemas de votación: máquina de palanca, tarjetas perforadas, papeletas de votación con o sin sistema de escaneo óptico y máquinas de grabación electrónica directa" (Euskadi.eus, 2021).

Actualmente, estos métodos de votación se mantienen en uso por la población estadounidense destacando entre los más usados el método de voto electrónico, “en las elecciones presidenciales de 2012 este método de votación alcanzo un uso del 40% es decir casi la mitad de la población de estados unidos utilizo este método para votar” (Euskadi.eus, 2021). En los últimos años se ha ido un poco más allá y por ejemplo para “las elecciones de 2018 el estado de Virginia Occidental lanzo un programa piloto con tecnología Blockchain en dos condados que permitía a los ciudadanos a los ciudadanos que estaban en el extranjero o en el ejército votar” (Euskadi.eus, 2021).

- Venezuela: “Desde 1998 se empezó a implantar el método por voto electrónico en este país, logrando en 2004 implementar un sistema completo, donde las personas podían ir a ejercer su voto a través de pantallas táctiles, imprimir su voto y depositarlo en unas urnas” (Euskadi.eus, 2021),

Así pues, en este país se ha visto señalado este método de votación por posible fraude, se ha solicitado auditoria de países como Estados Unidos, Chile, Colombia, etc.

En Asia los países que tienen un sistema de voto electrónico implantado son:

- Emiratos Árabes Unidos: “Desde 2006 se ha empezado a implantar el sistema de voto electrónico” (Euskadi.eus, 2021), con el fin de que las personas jóvenes ejerzan su derecho al voto en forma masiva, se ha tenido tanto interés en esto que por redes sociales el comité electoral ha lanzado campañas de pedagogía del buen uso del sistema para las votaciones, van guiadas especialmente hacia las personas más jóvenes.

  “Dado que el 88% de la población total es extranjera y la población es joven se decidió implantar las tecnologías más punteras con el fin de facilitar los trámites administrativos” (Euskadi.eus, 2021). Por eso, en mayo de 2013 los líderes de los EAU establecieron el objetivo de que en unos años todos los servicios públicos deberían ser accesibles a través de dispositivos móviles. “En 2015 se celebraron elecciones al Consejo Federal Nacional en las que sufragaron 224.000 personas, siendo la tasa de participación ciudadana de un 35%” (Euskadi.eus, 2021). En este proceso electoral que se desarrolló a nivel nacional totalmente electrónico “se registró un aumento del 119% en la participación, la población femenina también tuvo un aumento en participación” (Euskadi.eus, 2021). Así mismo, se conocieron resultados en un tiempo record que apenas superó los 30 minutos.

- Filipinas: Como se expone en Euskadi (2021), desde el 2007 se empezó a implantar el método de votación electrónica, en el 2008 se realizaron pilotos con urnas electrónicas y voto biométrico y para las elecciones del 2010 se realizaron las elecciones con el método de voto electrónico, pero se recibieron denuncias por fallos con las maquinas.

  En 2013 se volvieron a realizar elecciones legislativas con el mismo sistema de voto electrónico que en el 2010 y esta vez no se recibieron incidentes. “En las elecciones generales de 2016 se volvió a utilizar voto electrónico con 92509 máquinas electrónicas para 55 736 801 votantes” (Euskadi.eus, 2021), y por primera vez las maquinas emitían un impreso con el fin de poder validar el voto.

- India: “Desde 1989 comenzó de forma gradual la utilización del voto electrónico, y para el 2003 fue la primera vez que el 100% de los votos se emiten electrónicamente” (Euskadi.eus, 2021). Una década después, para las elecciones generales de “2014 se incorporó en el sistema de votación electrónica un nuevo método de verificación” (Euskadi.eus, 2021), ya que en las votaciones anteriores no se tenía como comprobar el voto, en el 2019 para las elecciones generales el 100% de las máquinas de votación incorporaron el comprobante de auditoria de papel verificado por el votante.

2.2.3 *Ventajas del método de voto electrónico*

El método de voto electrónico tiene muchas ventajas y si se tiene una pedagogía adecuada tiene gran aceptación, a continuación, se nombran algunas de las ventajas que el método por voto electrónico, según el sitio web de Evoting, tiene:

- Fácil adaptabilidad y uso, hoy en día gran parte de personas en el mundo cuentan con dispositivos electrónicos y “este método hace que sea más familiarizado y simple” (Evoting, s.f.), además hace que las personas jóvenes voten en mayor medida.
- En un sistema bien implementado la auditoria es sencilla y la entrega de resultado puede ser más rápida, con casos puntuales de tan solo 30 minutos después de cerrar las votaciones ya se conoce el resultado.
- En algunos países en donde utilizan el método de voto electrónico también tienen habilitado el voto por internet, haciendo que la facilidad para votar sea mayor y así contar con una mayor participación de los votantes.
- El ahorro de papel y materiales utilizados para votar de forma tradicional se ahorra, ayudando en cierta medida con el cambio climático.
- La facilidad en tiempo y desplazamiento para votar es notable con este método ya que si está habilitado se puede hacer desde cualquier lugar.

2.2.4 *Desventajas del método de voto electrónico*

Este método de voto electrónico trae muchos beneficios, pero no es un sistema de voto perfecto y tiene algunas desventajas, que se enuncian en Evoting (n.f.), las cuales se nombran a continuación:

- No es un sistema 100% seguro ya que tiene vulnerabilidad de seguridad y manipulación de la información.
- En algunos países o lugares se puede dificultar que las personas voten por este método ya que no todo el mundo tiene acceso a la tecnología o dispositivos móviles como celulares o computadores para poder votar.
- En algunos de los casos tiene un alto costo económico.

2.3 Método de Voto con Tecnología Blockchain

El método de votación con la tecnología Blockchain se ha vendido implementando y desarrollando en algunos países y lugares del mundo, uno de los más representativos o caso en el que se utilizó para unas elecciones en un escenario real fue en el 2018 para unas elecciones presidenciales en el continente de África, exactamente en el país de "Sierra Leona, después de 10 años de mandato del presidente saliente se desarrollaron unas elecciones presidenciales en donde la tecnología Blockchain fue la protagonista" (Beamonte, 2018), la empresa encargada de llevar a cabo estas elecciones se llama Ágora, y como afirma el artículo de Beamonte (2018):

> "Es una Startup Suiza, el objetivo principal que se tiene al desarrollar unas elecciones basadas en la tecnología Blockchain es reducir los costos de una votación recortando papeletas o tarjetones de papel, así como reducir la corrupción en el proceso de los comicios".

Su sistema de votación digital usa una cadena de bloques privada para supervisar los resultados en tiempo real. "Incluso los publico dos horas antes que la Comisión Nacional Electoral de la nación africana, con un recuento del 86%" (Beamonte, 2018).

La empresa Ágora se asoció con la Comisión Europea para ayudar a los operadores del nodo Blockchain provenientes de la Cruz Roja, el Instituto Federal Suizo de Tecnología y la Universidad de Friburgo. Al concluir la votación, "el equipo de 280 observadores acreditados ingreso manualmente alrededor de 400.000 papeletas en el sistema Blockchain de Ágora" (Beamonte, 2018). Después, los datos fueron transmitidos a las personas encargadas de supervisar y verificar el proceso democrático de la nación.

2.3.1 *Blockchain en las votaciones:*

La tecnología Blockchain se puede utilizar para realizar procesos de votación transparentes. Con un sistema de votación basado en Blockchain se puede eliminar muchos intermediarios, actualmente como funciona en gran parte de países en donde

votan de manera presencial y tradicional se selecciona a personas naturales para que ejerzan como jurados, sin verificar un perfil y sin comprobar una capacidad específica para ejercer el cargo, y son seleccionados aleatoriamente miles de jurados. “Usando la tecnología Blockchain cada ciudadano puede enviar su voto anónimo a la cadena de bloques, además, los resultados de las votaciones al quedar registrados no se pueden modificar” (MinTic, 2020); esto elimina la sobrecarga considerable del entorno de votación, desde la preparación hasta la tecnología, el personal y los recuentos.

Acá en Colombia se desarrollaron algunos ejercicios electorales en algunas instituciones educativas de la ciudad de Bogotá para elegir el personero; además, se realizaron en conjunto entre la Alcaldía Mayor de Bogotá y ViveLab de la universidad Nacional de Colombia, ellos usaron un sistema basado netamente en la tecnología Blockchain con resultados completamente exitosos, la escalabilidad de estos ejercicios fue mucho menor a unas elecciones a nivel nacional para un país completo, pero a nivel de laboratorio y demostración de la funcionalidad de la tecnología fue destacable.

2.3.2 *Ventajas del método de voto con tecnología Blockchain*

Este método es tecnológico o con mucho aporte de tecnología y un usuario normal que ya tenga la experiencia votando de forma electrónica no tendría una gran diferencia en cuanto a la experiencia de usuario al realizarlo utilizando la tecnología Blockchain, un usuario que siempre ha votado de forma tradicional si tendría una experiencia de usuario totalmente diferente, entre estas tres formas de voto electrónico lo que cambia es la tecnología que se usa por debajo para el funcionamiento del método.

A continuación, se nombran algunas de las ventajas del método de voto con la tecnología Blockchain:

- Experiencia de usuario a la del método de voto electrónico.
- Amigable con el medio ambiente en cuanto al ahorro de material como papel, cartón, tintas, etc.
- Mayor seguridad y trazabilidad del voto del usuario.
- Las características propias de la tecnología.
- Es un sistema de fácil auditoria, haciéndolo un sistema transparente.
- Mayor facilidad al voto porque se puede realizar desde un dispositivo electrónico sin necesidad de desplazarse a un lugar de votación.

2.3.3 *Desventajas del método de voto con tecnología Blockchain*

Blockchain aplicado a votaciones electorales siempre se ha planteado como la tecnología ideal y que sería un sistema perfecto, y pueda que, si se tenga razón en esto, pero la tecnología no deja de ser muy nueva y genera incertidumbre, por ende, hasta el momento se tienen algunas desventajas que tiene la tecnología Blockchain para el uso de votaciones electorales y se exponen a continuación:

- ❖ Falta de regulación de la tecnología
- ❖ Es una tecnología nueva, muchos de los expertos tecnológicos dicen que apenas se ve la punta del Iceberg.
- ❖ La falta de conocimiento, pedagogía y socialización con las personas, hacen que les genere escepticismo.
- ❖ En países como Colombia sería difícil el acceso al voto de esta forma, porque no todas las personas cuentan con un dispositivo electrónico.
- ❖ La falta de personal capacitado o con el conocimiento profesional para liderar y llevar a cabo unas elecciones a nivel nacional basadas en la tecnología Blockchain.

2.4 Cuadro Comparativo

Tabla 1. *Cuadro comparativo: voto tradicional, voto electrónico y voto Blockchain*

	Voto Tradicional	**Voto Electrónico**	**Voto Blockchain**
Costo	Es un método costoso y no amigable con el medio ambiente porque utiliza mucho material como papel, tinta, cartón, etc. Los costos también se elevan por la gestión y cubrimiento que debe realizar para cubrir un país completo.	Es un método costoso, pero menos en comparación al voto tradicional, ya que reduce costos en materiales y en gestión de personas que deben participar en las elecciones. Hay países como Brasil que alquila las máquinas de votación a otros países.	En este método los costos son parecidos al método del voto electrónico, y menor al costo que tienen unas elecciones de forma tradicional.
Transparencia	El voto de cierto modo no cumple con la transparencia porque una vez lo ejerces pierdes toda la trazabilidad de este.	En este método se ha tratado de que las personas impriman un comprobante de su voto para mejorar la transparencia de las elecciones pero tiene muchos críticos porque un voto debe ser secreto.	Es un método totalmente transparente porque las personas pueden realizar el seguimiento a su voto y verificar que este efectivamente este en la cadena de bloques y sea contado. Con el hash de la transacción lo puede realizar el proceso que se menciona anteriormente.

Seguridad	Es un método que está expuesto a fácil manipulación de votos, cumple con una cadena muy grande en donde los votos pueden ser alterados, o el sistema de conteo (software) también puede ser vulnerable.	Es un sistema que funciona bien, pero puede ser atacado y perder información o que esta sea modificada con un fin. El sistema de seguridad, certificador de voto, y sistema auditable hacen que los costos de la solución suban, pero son necesarios para garantizar las elecciones.	Es un sistema seguro en el Core del sistema que es con la tecnología Blockchain, la información no se puede manipular ni cambiar a conveniencia, haciendo este método más seguro en cuanto a la conservación de los votos originales por los votantes.
Facilidad	Es un método fácil y al que pueden acceder y votar muchas personas, es un método muy intuitivo en el que únicamente en una hoja de papel se selecciona el candidato de su elección. Se complica en cuanto al desplazamiento que tengan que realizar las personas al punto de votación, porque pueden ser lugares muy distantes, de difícil acceso o la persona tiene algún limitante físico que le impida desplazarse.	Es un método en donde se tiene interacción con tecnología o con una máquina, pero de igual forma puede ser algo intuitivamente sencillo para una persona votar. Existirán personas que les cause terror votar de esta forma y más si no están acostumbradas y lo hacen por primera vez, si tiene habilitado el voto por internet y no únicamente de forma física se libraría del problema de que las personas deban desplazarse al lugar de votación.	En cuanto a la facilidad es muy parecida a la del método de voto electrónico ya que el usuario interactúa con una pantalla en un punto de votación o desde un dispositivo móvil, para el usuario final sería muy intuitivo poder ejercer su derecho al voto.
Gestión	Para realizar unas votaciones de la forma de método tradicional se necesita realizar una gestión muy grande y la cual	Para realizar unas votaciones a nivel nacional con el método de voto electrónico en muchos lugares del mundo	Para realizar unas votaciones a nivel nacional con Blockchain únicamente necesitaríamos de

	depende de muchas personas para que funcione.	tienen sus propias máquinas de votación, la necesidad de tener muchas personas en el proceso disminuye, pero la gestión para la distribución, funcionamiento y mantenimiento de las máquinas.	poder computacional, se pueden instalar unos computadores en algunos puntos físicos para las personas que decidan ir a votar en estos lugares, pero es válido señalar que todas las personas pueden votar desde cualquier dispositivo móvil, computador, Tablet.
Manipulación	El método tradicional está más expuesto y sujeto a manipulación de los votos para un fin. A pesar de la enorme gestión que se realice, los votos podrían ser fácilmente manipulados en varias partes del proceso.	El método de voto electrónico puede ser manipulado en cuanto a que sufra algún ataque cibernético de manipulación de la información. Tiene más dificultad que puedan realizar un ataque de esta forma efectivo, aun así la posibilidad de ataque esta.	Muchas personas especializadas en sistemas y métodos de votación opinan que la tecnología Blockchain es la ficha del rompecabezas que hace falta para tener un sistema de votaciones ideal. Y es que la tecnología Blockchain no puede ser manipulada, cualquier cambio en alguna de las transacciones (votos) quedara expuesta ante todos los observadores, siendo un sistema o tecnología anti-manipulación.
Auditoria	Es un sistema el cual es auditable pero lento, ellos deben verificar que todo el proceso y los votos que se dictaminaron en el resultado sean verdaderos, deben	En el sistema de voto electrónico la auditoria es un poco más rápida pero igual lleva un proceso largo en la validación y verificación de las máquinas de votación.	El método de voto con tecnología Blockchain cuenta con un sistema auditable rápido y transparente, puede ser auditado directamente por el usuario o votante si

	realizar reconteo de votos y verificación de procesos.		así quisiera.
Implementación	Este método al ser el más antiguo y usado en la gran mayoría del mundo cuenta con una estructura de implementación avanzada. Es válido aclarar que cada vez que se van a realizar unas elecciones de este tipo la gestión para desplazar los materiales y organizar a las personas que participan es un trabajo enorme y que requiere de mucho tiempo antes en empezar con la organización para el día de las elecciones.	El método de voto electrónico tiene implementación más sencilla porque dispone de una cantidad mucho menor a materiales y a personas, lo que hace que su implementación sea más rápida y que no necesite disponer de tanto tiempo de anterioridad para la gestión de las elecciones. Para este método demoraría más en la distribución de las máquinas de votación y alistamiento de la red tecnológica.	Para el método con la tecnología Blockchain el proceso de implementación es parecido al del método de voto electrónico, pero más sencillo a la distribución de equipos ya que no se requiere de equipos especiales para votar. Una vez se tenga el protocolo de red e infraestructura tecnológica funcional, el tiempo de implementación será el de alistar los puntos que se habiliten para votar, también se puede votar a través de internet ahorrando tiempo de implementación de los lugares de votación.
Trazabilidad	Para el votante tener la trazabilidad de su voto en este método es muy complicado, de hecho no se tiene y debe dejárselo todo a la confianza del sistema de votación.	La trazabilidad del voto bajo el método de voto electrónico es posible siempre y cuando la maquina imprima un comprobante del voto del usuario, pero esto no es permitido o habilitado legalmente en todos los países en donde se vota electrónicamente.	Con el método de voto con la tecnología Blockchain si existe la opción de que las personas tengan la trazabilidad de su voto, lo busquen y validen que este dentro de la red y que este efectivamente sea contado.
Uso actual	Este método	Es el segundo método	Es el método menos

	actualmente es el más usado a nivel actual, pero con muchos señalamientos acerca de su funcionamiento y veracidad.	más usado actualmente y cuenta cada vez con mejoras es sus procesos y tecnología.	usado actualmente, se conocen de investigaciones de países grandes e importantes para su uso, y es el método y tecnología que más promete en cuanto a un método de y procesos de votación.

Nota. Fuente del análisis: el autor.

3. Diseño de la Gestión del Sistema electoral

En este capítulo se realizará el Diseño de la red pensada para un ejercicio electoral presidencial o de alcaldes a nivel nacional. En este capítulo no únicamente se encontrará un esquema con el diseño de la arquitectura, sino que también se encontrará con todos los aspectos relacionados a los términos, actores y fases que componen una acción o evento de esta magnitud que son relevantes y hacen parte del diseño en general de la red.

3.1 Diseño Funcional de la Solución

El diseño funcional de la solución se desarrollará teniendo en cuenta todas las tecnologías ya existentes. El objetivo se basa en proponer una solución de voto telemático que incluya las soluciones de la tecnología blockchain y de esta forma garantizar un sistema más transparente y seguro.

Esta solución propuesta por la Alcaldía Mayor de Bogotá (2017), cuenta con todos los requisitos generales que debe tener una votación, como los de las votaciones electrónicas, y además debe cumplir con los siguientes requisitos fundamentales para nuestra solución:

1. *Transparencia:* debido al mecanismo de consenso, “la información se hace consistente y con reducción de errores, esto permite conocer el detalle de cada transacción y de los participantes +0 +de la misma” (Alcaldía Mayor de Bogotá, 2017). Para un proceso electoral, esto consolida la construcción de confianza ciudadana basada en la transparencia y no en la reputación. Debe ser un sistema totalmente transparente en aspectos como el software (que algoritmos se usan, cual es la solución, etc.) e información (cualquier persona interesada en cualquier momento podría acceder a los datos de la votación).

2. *Seguridad:* la criptografía hace la seguridad del sistema “gracias a los complejos procedimientos criptográficos, los cuales permiten garantizar la autenticidad de la información” (Alcaldía Mayor de Bogotá, 2017). Esto hace indispensable a la criptografía como parte del sistema.

   Debido a su estructura de funcionamiento de autoprotección, en donde la generación de nueva información es el producto de una línea coherente de bloques previos combinando las transacciones nuevas, ya que según el informe de la Alcaldía Mayor de Bogotá (2017) sobre este tema indica que, cualquier intento de añadir transacciones nuevas sin conocer la información de los bloques anteriores, evita que información corrupta se agregue al bloque.

Que “un bloque sea inalterable brinda la salvedad de la información que contiene ese bloque” (Alcaldía Mayor de Bogotá, 2017). Estas dos características de seguridad encajan exactamente para que en una actividad electoral se garantice la seguridad de la misma.

Para garantizar una actividad electoral justa y exitosa la solución debe ser segura y robusta, resaltando que exista posibilidad de uso masivo en intervalos cortos de tiempo, asimismo no debe permitir la modificación o eliminación de votos emitidos por otros usuarios, y finalmente no debe permitir alteraciones de la votación (ataques DDOS, ataques de interrupción al flujo de votación, etc.).

3. *Descentralización:* La descentralización es una característica de funcionalidad de la tecnología blockchain y para el caso del sistema que se quiere diseñar es muy apropiada. Esta característica permite múltiples nodos trabajando en paralelo y no que todo el proceso “se gestione en un solo nodo, estableciendo que la confianza no recaiga únicamente en un nodo, si no en el sistema global como tal” (Bermúdez, 2016).

4. *Flexibilidad:* la flexibilidad de la solución debe ser amplia ya que el sistema debe funcionar en diferentes situaciones o aspectos de la votación.

Algunos ejemplos de aspectos de la votación, según Bermúdez (2016) que se permitan configurar en la solución son:

a. Posibilidades del voto:

- ❖ voto directo a un candidato(a): son las votaciones válidas para Elección Presidencial. Son del tipo de votación en la que el voto es válido para una única opción.
- ❖ voto directo a varios candidatos: son las votaciones válidas para elección de Alcaldes, Gobernadores, Senado. Son el tipo de votaciones en las que se selecciona más de una alternativa es decir que el voto es válido para más de una opción, por ejemplo, voto para el senado: candidato(a) y partido político o voto para: elección de alcaldes y gobernadores.
- ❖ otros, son tipos de votaciones ajustables a la necesidad del usuario como por ejemplo unas votaciones para una junta directiva, o elecciones en las que la transparencia, seguridad y confiabilidad sea lo estrictamente necesario.

a. Gestión del voto: para la solución pensada en este proyecto aplica que el voto se pueda delegar o que se necesite presencia de otro votante por ejemplo un mayor de la tercera edad que puede votar pero que está limitado físicamente para hacerlo.

Así mismo, puede ser bajo la modalidad de voto mixto es decir que combina el voto telemático y voto presencial por ejemplo para unas votaciones en las cuales a las personas que por limitaciones físicas no puedan trasladarse o que se encuentren en el extranjero, puedan ejercer su voto de manera virtual y se cuente igual que un voto presencial.

b. Segmentación del voto: los votos para el conteo y estadísticas se hará geográficamente cómo se desarrolla actualmente en el país, es decir, se agrupan y cuentan por ciudad.

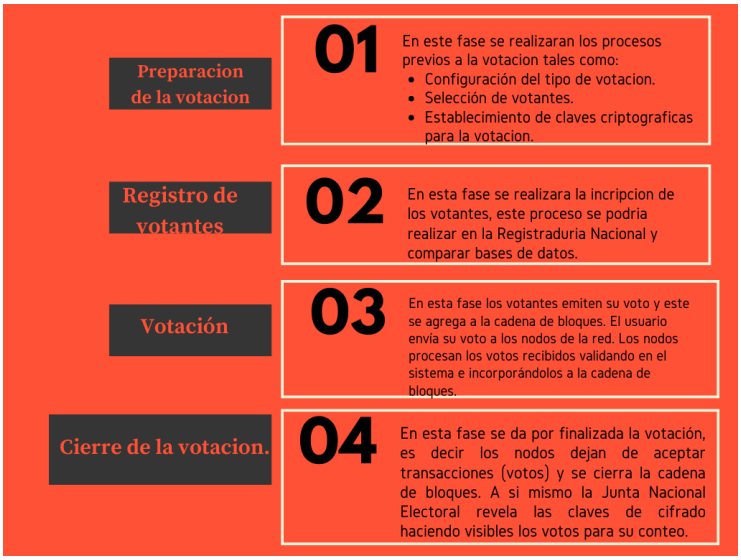
3.1.1 *Fases de la Votación*

La solución propuesta está enfocada a todo el ciclo de vida de una elección presidencial en el territorio colombiano. El cubrimiento de la solución abarca desde la preparación de la votación hasta el recuento final de los resultados.

En parte a que este ejercicio electoral es específico en cuanto al territorio (país, ciudad, lugar) y tipo de votación, y como se ha nombrado anteriormente también se puede ajustar a cualquier tipo de votación claro está que, con sus pertinentes cambios, lo cual la hace una solución flexible.

En la siguiente imagen, figura 7, se muestran las fases de la solución con sus respectivos procesos, todo el ciclo de vida de las votaciones se distribuye de forma consecutiva, es decir, que conlleva un orden y que de la finalización de una fase conlleve a la iniciación de la fase siguiente. Cada uno de los procesos que se llevan a cabo son diferentes y todos juntos corresponden a la gestión de la red.

Figura 8. *Fases de la Solución*



Nota. Fuente: el autor.

3.2 Actores

A lo largo de las votaciones intervienen unos actores que son de importancia para su control y funcionamiento, a continuación, se detallan:

1. Votante: Son las personas que participan en la votación emitiendo un voto.
2. Organismos de control: Son los organismos encargados de velar administrativamente por el evento. Estos son la Registraduría Nacional del Estado Civil y el Consejo Nacional Electoral (Wikipedia, 2021).
3. Nodos: Son todos los nodos en los que se esté ejecutando la solución, pueden ser personas u organizaciones interesadas que instalen el software. Estos nodos tendrán dos funciones:
    1. Replicar la base de datos blockchain, asegurando la seguridad y la integridad de los votos.
    2. Según sean los votos recibidos generar nuevos bloques que se agreguen a la cadena blockchain.

Los nodos también son parte fundamental para la auditoría de la red ya que cualquier persona u organización que esté autorizada, únicamente tendrá que establecerse como uno de estos nodos, y monitorizar la cadena de bloques blockchain que contiene los votos. Serían nodos pasivos es decir que forman parte de la red y por lo tanto de la seguridad pero que no generan nuevos bloques (aunque si quisieran podrían generar nuevos bloques).

3.2.1 *Preparación de las elecciones*

Las votaciones o el evento tienen una fase inicial la cual es su preparación y es en donde se especifican los parámetros bajo los cuales funcionará la votación. Para lo cual se deben realizar las siguientes tareas, tal y como se recomienda en el documento de Bermúdez (2016):

- Generar las claves de la elección: Los organismos de control crearán dos claves criptográficas una pública la cual será publicada y una privada la cual será dividida y repartida entre funcionarios de los organismos de control. “Estas dos claves son necesarias para el cifrado de los votos y dado que la clave privada está dividida entre algunos miembros” (Bermúdez, 2016), se necesita de la presencia de todos estos miembros para el cifrado y recuento de los votos.

- Definición de la votación: Aquí se establecen los términos bajo los cuales será el funcionamiento de las votaciones.
  A continuación, se darán algunos ejemplos, basados en los expuestos en Bermúdez (2016):

- “Votantes. Por ejemplo, que todos los ciudadanos autorizados para ejercer el voto sean mayores de edad.
- Agrupación de votos. Por ejemplo, la agrupación por ciudad o departamento y luego realizar la suma del ponderado total.
- Tipo de votación. Por ejemplo, el valor representativo del voto, si es para presidente únicamente será válido para un candidato” (p.48).

- Generación del resto de claves y elementos necesarios para la votación:
  - Direcciones de votación. Son las direcciones correspondientes al envío de los votos, es decir las direcciones a donde va y se aloja el voto del usuario. Por ejemplo, “para unas votaciones presidenciales a nivel del país, pueden existir direcciones para cada ciudad o municipio, de esta forma los votantes emitieron su voto a la dirección donde tengan autorizada la votación y el recuento se hará agrupando por direcciones (ciudades, departamento o municipios)” (Bermúdez, 2016).
  - Certificado de firma de la entidad validadora. Es necesario un certificado por cada agrupación de votos, para este caso la entidad validadora es la Registraduría Nacional.
  - Algoritmos de firma y cifrado que se utilizarán.

3.3 Registro de Votantes

Para garantizar un proceso de voto de calidad la planificación del mismo lleva a deducir que para participar y acceder a la votación es necesario que el usuario se registre previamente, es decir que existe una etapa previa a las votaciones la cual es el registro de los votantes. De esta manera se podrá comprobar la identidad de cada votante.

Para garantizar la transparencia del proceso el votante, según Bermúdez (2016):

“Se debe cumplir con unos requerimientos necesarios los cuales hacen parte del funcionamiento de las elecciones tales como:

- Puede votar ya que cumple con los requisitos válidos para la votación (edad, nacionalidad, etc.)
- El votante únicamente podrá emitir un voto.
- No será posible vincular el voto con la identidad del votante” (p.49).

Este sistema contará con dos fases en aras de conseguir el resultado, estas dos fases están diferenciadas, es decir son independientes debido a que se realizan en momentos distintos, también se debe tener en cuenta que de la primera fase que es el registro depende la segunda fase que es la votación.

Figura 9. *Fases de Votación*

Nota. Representación de las fases de votación inspirada del texto guía de Bermúdez (2016). Fuente: el autor.

3.3.1 *Etapa 1: Registro de los usuarios.*

Para el desarrollo de esta fase es indispensable que todas las personas que estén habilitadas para votar realicen un registro, esta información que proporcionan es de gran importancia debido a que el usuario solicita la dirección de votación o clave pública de la misma, este proceso se realiza entre dos software, uno es con el que interactúa el usuario y realiza una solicitud de la dirección que apunta al sitio de la votación, “el software de servicio del registro puede ser que sea administrado por la junta electoral” (Bermúdez, 2016) o en este caso de la Registraduría Nacional de Colombia, después de recibir la solicitud de registro y de dirección de votación, esta se valida, comprueba y confirma y posteriormente se envía desde el software de servicio de registro un comprobante de habilitación del voto al usuario, este comprobante certifica que la información es verídica, que la persona está habilitada para votar, y que el registro fue satisfactorio.

3.3.2 *Etapa 2: Votaciones.*

En la fase dos el procedimiento es diferente, el usuario llega el día de la votación y desde el software del usuario envía el comprobante al software de servicio de registro que recordemos puede ser la misma junta electoral, estos reciben el comprobante, se valida y confirma que la persona está habilitada para votar y se le asigna el voto justo en ese momento por medio de una credencial, allí estarán alojadas las claves criptográficas para realizar el voto. Dado que, para habilitar la credencial con el voto se presenta un comprobante anónimo, no se podrá asociar la persona que vota o su credencial con el

voto emitido permitiendo que se lleve a cabo unas elecciones transparentes y totalmente auditables.

El proceso se realiza en dos fases y no se hace todo desde la fase uno, debido a que, “un atacante puede rastrear la asignación del voto haciendo vulnerable el sistema” (Bermúdez, 2016), si se hace de esta forma un atacante no puede rastrear u obtener alguna información de la red o del sistema ya que el voto se habilita momentos antes de que el usuario vote.

3.4 Fase de Votación

En esta fase se explica y profundiza acerca del proceso de votación, tomando como base los apartados de “fase de votación” en el documento de Bermúdez (2016), ya que al usuario votar se procesan varias transacciones con una dirección de destino y su correspondiente firma digital que se explicarán a continuación:

- *Transacción de Inicio:* se conoce como la transacción de entrada, con la cual se habilita el voto para el usuario, es decir que es la transacción que se genera cuando al usuario se le entrega la credencial con el voto habilitado para las elecciones.

    - *Transacción de salida:* este tipo de transacción se genera cuando el usuario realiza su voto, es decir, vota por su candidato favorito, para esta parte se utiliza la clave pública de la votación la cual será generada y otorgada por la junta electoral; es válido aclarar que este proceso no se realiza para conservar el anonimato del votante dado que con el sistema de entregar las credenciales del voto antes de votar ya se garantiza, pero al cifrar los votos también se garantiza que mientras se estén realizando las elecciones no se puedan obtener ningún tipo de resultados previos, “el resultado total se conoce al final cuando la junta electoral revele la clave privada para descifrar los votos y realizar el conteo” (Bermúdez, 2016).

      En otro proceso que “va dentro de la transacción de salida, pero aparte del cifrado del voto se realiza el cargue de votos hábiles” (Bermúdez, 2016), para ser más precisos esto funcionara en los casos de que sean unas elecciones por ejemplo de congreso en donde la persona tiene varios votos, si esto lo ponemos en paralelo a una votación normal es decir con papeletas, sería que si son unas elecciones para elegir presidente únicamente se entregará un tarjetón y podrá elegir un único candidato para que el voto cuente, en otro caso sería para congreso, alcaldes y gobernadores en donde al usuario se le entregan varios tarjetones y este vota más de una vez, en este caso sería exactamente lo mismo, dependiendo del tipo de elecciones se cargan uno o la cantidad de votos hábiles.

      Este proceso también se podría realizar en conjunto con “el proceso de cifrado, pero si se mantiene por separado se asegura que el usuario no realice

más votos de los que puede efectuar" (Bermúdez, 2016) y si esto ocurriese desde el mismo momento que el usuario realice más votos de los posibles se le informa que esto no es posible ya que la red realizó la validación antes de ser agregada a la cadena de bloques y en lugar de que al final cuente como un voto nulo simplemente le va a decir desde el comienzo que su voto no ha sido efectivo ni válido por esta razón.

- *Dirección de Destino:* esta dirección de destino es la misma en donde se agrupan los votos a la hora de la votación, "esta dirección puede ser la misma del colegio electoral, registraduría de la nación o la junta electoral" (Bermúdez, 2016). Al estar agrupados los votos se genera mayor confianza y también para el conteo de los mismos sería más sencillo.

- *Firma digital:* la firma digital aporta la seguridad y la confianza que el usuario puede y tiene derecho a votar y hacer uso de la transacción base de la elección, esta firma digital viene en la transacción por medio de las credenciales de votación.

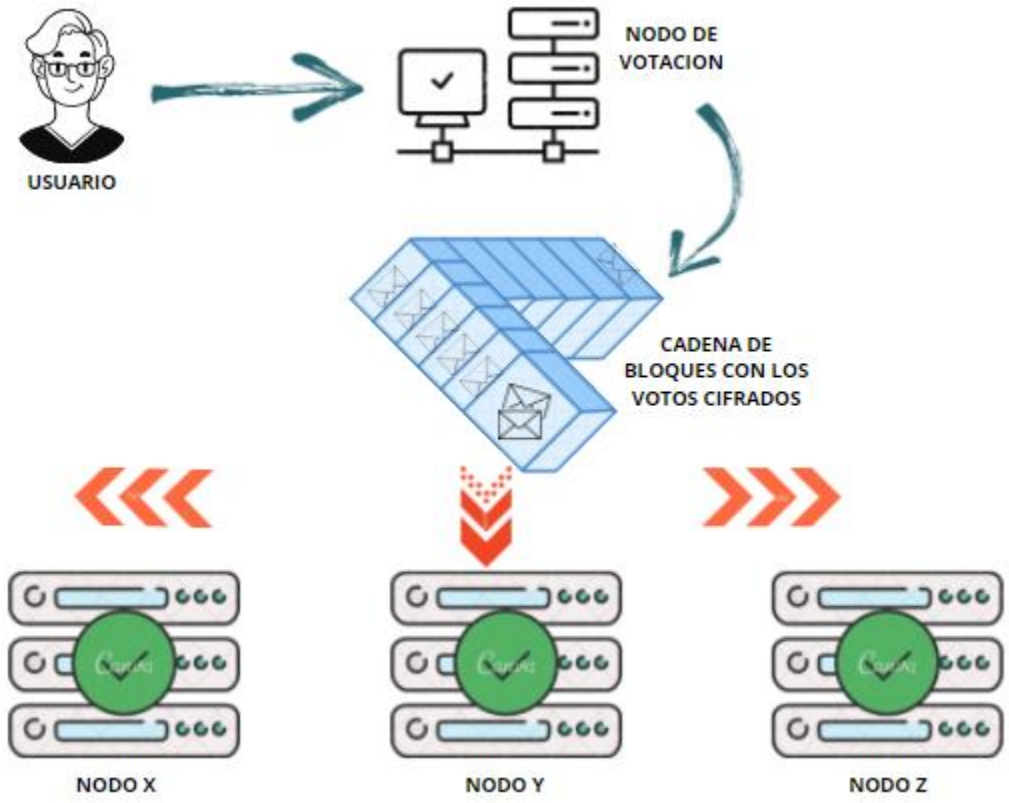
Los nodos de la red son los encargados de recibir y procesar las transacciones, según el trabajo de Bermúdez (2016), estos las validan y procesan realizando dos acciones que se explican a continuación:

1. *Validación de las transacciones:* para que un nodo apruebe la transacción y la agregue a uno de sus bloques primero revisa lo siguiente:
    a. "Que la estructura de la transacción sea la correcta" (Bermúdez, 2016), es decir que cumpla con la estructura de transacciones de votos que se define por la junta electoral.
    b. Como se mencionaba anteriormente, se verifica que la firma digital es auténtica al igual que las credenciales de voto las cuales certifican que el usuario en cuestión está habilitado para votar.
    c. La suma de los votos emitidos por el votante no debe superar la cantidad de votos habilitados por la junta electoral en el momento de la entrega de la credencial que son los mismos votos habilitados en la transacción base (tarjetón).
    d. "La dirección de destino que se le asigna al usuario para la votación debe ser válida" (Bermúdez, 2016), es decir, que apunte para el lugar correspondiente, en este caso como la red es para unas votaciones a nivel nacional se requiere y se comprueba que la dirección de destino sea de la ciudad o zona a la cual el usuario pertenece y se inscribió para la votación, esta validación se realiza a través de la credencial ya que dicha dirección se carga a esta y será hábil solo para el mismo lugar o ciudad al que el usuario pertenece.

2. *Inserción de bloques en la cadena de bloques de la votación:* los nodos de la red según vayan aprobando las transacciones y estas se vayan agregando a los bloques agregan los bloques nuevos a la cadena de bloques de la elección (Bermúdez, 2016).
3. *Propagación de los bloques:* el nodo que quiera agregar un bloque con las transacciones de este mismo bloque, lo agrega y difunde a todos los demás nodos de la red, de esta forma se cumple con el principio de red distribuida, ya que “esa información no va a estar solo en el nodo que agrega el bloque, sino que va a estar en toda la red blockchain electoral” (Bermúdez, 2016).

A su vez, “como es una red pública el usuario o votante va poder confirmar que su voto efectivamente está en la red y que va a contar en su momento” (Bermúdez, 2016), vale aclarar que ningún usuario puede ver el contenido del voto porque los mismos están cifrados, lo que pueden ver es su voto por medio de una transacción que se agregó a un bloque y este a la red electoral.

Figura 10. *Proceso de Votación*



Nota. Inspirada en el texto guía. Fuente: el autor.

En resumen, como se puede ver en la imagen anterior, figura 9, en el momento de la votación y cuando el usuario vote por su candidato se verifica la credencial del voto y la

dirección de destino, después el usuario envía el voto al nodo de votación, este válida la transacción o voto para este caso y la agrega a un bloque, este bloque se agrega a la cadena de las elecciones y posteriormente se comparte la actualización en la cadena de bloques con todos los nodos de la red.

3.5 Finalización y Conteo de Votos.

En la finalización de las votaciones la junta electoral o Registraduría Nacional, en el caso colombiano, envía un último bloque, este último bloque se utilizará como señalización indicando que a partir de ese bloque no se contarán más votos, es decir, los votos que están en las transacciones de los bloques anteriores al final serán los votos contabilizados para determinar el resultado final de las elecciones. A partir de ese momento los nodos ya no emitirán ni recibirán más bloques a la cadena de bloques de las elecciones.

A continuación, cada apartado toma como base planteamientos realizados en el trabajo de Bermúdez (2016).

Cuando la junta electoral tenga la cadena de bloques definitiva y las elecciones ya están cerradas se debe:

- Recomponer la clave privada: la clave está distribuida a elección de la junta directiva de las elecciones a sus distintos miembros.
- La clave privada será compartida con aquel organismo, partido político, comunidad o personas que deseen auditar el proceso de conteo de votos.
- La clave privada se utilizará para descifrar los votos que están en las transacciones que están en la cadena de bloques de las elecciones.
- Se procesa la información, es decir se leen, cuentan y calculan los resultados de las votaciones.
- Se procede a publicar los resultados de las votaciones.

Las reglas dependen del tipo de elecciones que sean, junta directiva, congreso, alcaldes y gobernadores, presidencia de estado, etc. “lo importante es que estén claras y consignadas junto con el algoritmo desde la preparación de las elecciones, ya que de esto también va a depender el conteo de votos” (Bermúdez, 2016), porque se debe determinar cuáles y cuántos votos son nulos.

Un ejemplo de lo anterior, para unas votaciones de congreso se habilitan cinco votos pero si una persona utiliza los cinco votos para el mismo candidato es como si se le dieran cinco tarjetones pero marca un solo tarjetón cinco veces, el voto se contará como nulo, pero para unos comicios presidenciales como el que se plantea para este proyecto el voto nulo será más fácil de pre definir por el tipo de votación de único candidato lo

complicado y que será un tema en el que se profundizará más adelante es la escalabilidad del sistema.

Para esta etapa de las elecciones la clave privada es importante por las acciones y procesos que se realizan a través de ella, una que quiero resaltar es “la fácil auditabilidad de las mismas ya que al compartir la clave privada cualquier interesado o persona que quiera verificar que su voto fue correctamente contabilizado puede hacerlo” (Bermúdez, 2016). Permitiendo cumplir uno de los principios el cual es la transparencia gracias a que el sistema no es centralizado y si es un sistema distribuido y auditable.

3.6 Software

A continuación, se desarrollará un poco más acerca del software que se va a utilizar, para que la solución sea completa y como se va a nombrar la parte de infraestructura de equipos también se debe nombrar la parte de software para que enlace con la parte de infraestructura y tener una propuesta de solución más completa.

La demanda en el servicio ofreciendo los estándares mínimos de calidad de y de experiencia hacia los clientes.

3.6.1 *Software de Votación*

En este punto se tiene en cuenta los planteamientos base del documento de Bermúdez (2016).

Ahora bien, el sistema que se busca desarrollar profundiza en el software de votación que es el mismo con el que el usuario interactuara desde el registro, la solución que se desarrolla es de un voto 100% telemático pero también semi-presencial, el papel y las papeletas quedan obsoletas y las personas que voten en el centro de votación lo harán desde unos puntos habilitados en donde encontraran, computadores o tablets para que puedan hacerlo, lo que se resalta de este apartado es que el usuario de principio a fin tiene una gran interacción con el software.

Debe ser un software que sea sencillo e intuitivo para que las personas al momento de votar puedan hacerlo sin ningún problema, esta solución se puede realizar de varias maneras, puede ser una única aplicación o pueden ser varias aplicaciones y que se unan en un conjunto.

4. Solución Técnica del Sistema

Tipo de Red Blockchain elegida:

Se define o delimita el tipo de red bajo el cual será desarrollado el sistema de blockchain planteado para este proyecto.

La red ferada o híbrida es el tipo de red más seguro y que mejor se acomoda a un sistema de votación blockchain transparente, al ser una red híbrida tendrá una parte que es privada y otra que es pública.

4.1 Arquitectura Basada en el Documento Oficial de Ágora

Dentro del estudio se han realizado varias indagaciones acerca de cuál podría ser la mejor arquitectura para la red blockchain electoral a nivel nacional para este proyecto, teniendo en cuenta la escalabilidad de esta ya que en la mayoría de estudios y pruebas realizadas en el mundo son a escalas más pequeñas.

ÁGORA es una empresa que desarrolló su propio protocolo y arquitectura para que se realicen unas elecciones a mayor escala, seguras, confiables y transparentes durante todo el proceso, teniendo en cuenta esto se detalla este tipo de arquitectura que implementa ÁGORA (2021) y su funcionamiento, para que sea usada como ejemplo o incluso para que se tenga en cuenta esta empresa en el proceso de una futura implementación del proyecto.

La seguridad y transparencia son factores determinantes en un ejercicio electoral de esta magnitud por tal razón dentro de la arquitectura que se plantea se cuenta con dos tipos de nodos es decir utiliza una infraestructura de dos capas para el consenso que se combina con el nivel más alto de criptografía.

Seguido a esto, “una de las capas se compone por los nodos de validación o consenso de la red de bloques de la estructura de las elecciones” (Ágora, 2021), estos nodos son nodos operados por terceros certificados, tales como universidades, entidades gubernamentales y entidades internacionales, ellos serán garantes de la cadena de bloques. La otra capa se compone de los nodos de auditoría, la auditoría la puede realizar cualquier persona una vez finalice la votación y se den a conocer los resultados, pero también se va a tercerear es decir esta parte la realizara una entidad certificada y que se encargue de estos procesos de auditoría y de este modo intervenga y verifique que todo es correcto.

Se debe destinar unos fondos para comprar *tokens*, estos se utilizarán durante todo el proceso, por ejemplo, al final de la votación con estos se pagará a los nodos que participaron en las elecciones por su trabajo de procesamiento y verificación.

El sistema funciona a base de TOKENS, un *token* traducido al español significa ficha, y básicamente en el sistema funciona como ficha digital, moneda digital, o simplemente algo que guarda valor. “Los *tokens* son unidades que pueden representar diferentes cosas, dependiendo de cómo sean programados” (Bitcoin México, 2019).

La particularidad de los *tokens* que se utilizan en el mundo de las criptomonedas y blockchain es que son digitales. “No existen físicamente, sino que están programados sobre la Blockchain del protocolo que se usa para programar el token” (Bitcoin México, 2019).

Antes de entrar a desarrollar cada componente de la infraestructura que se propone se definirán algunos conceptos claves que se nombraran y utilizaran:

- *Junta electoral:* es la encargada de los comicios, quien contrata el servicio o en su defecto lo desarrolla, a nivel Colombia sería la Registraduría Nacional junto con las entidades del gobierno encargadas de desarrollar el proceso electoral.

- Tokens reservados para las elecciones: los *tokens* deben ser comprados según sea la decisión de la junta electoral, es decir, si la junta desarrolla todo el proceso deberán hacer la compra de los *tokens*, si el servicio es contratado, esta compañía será la encargada de comprarlos con una parte del dinero pactada que se estipule en un contrato. Estos serán utilizados para pagar a los nodos de consenso como a los de auditoría por sus servicios prestados durante todo el proceso de las elecciones electorales.
- *Nodos de consenso:* son unos nodos más específicamente una red distribuida de servidores que harán de testigos independientes, toda esta red de nodos será llamada “COAUTORITY” una red de nodos de consenso de autoridad y validación colectiva sobre la cadena de bloques de ÁGORA.
- *Nodos de auditor ciudadano:* es una red de nodos global descentralizada, estos nodos no se basan en la confianza de la red, es decir están ahí para precisamente constatar que todo es claro y transparente, toda esta red de nodos será llamada “VALEDA” la cual verifica que todo el proceso de consenso realizado por los otros nodos se procesa correctamente.

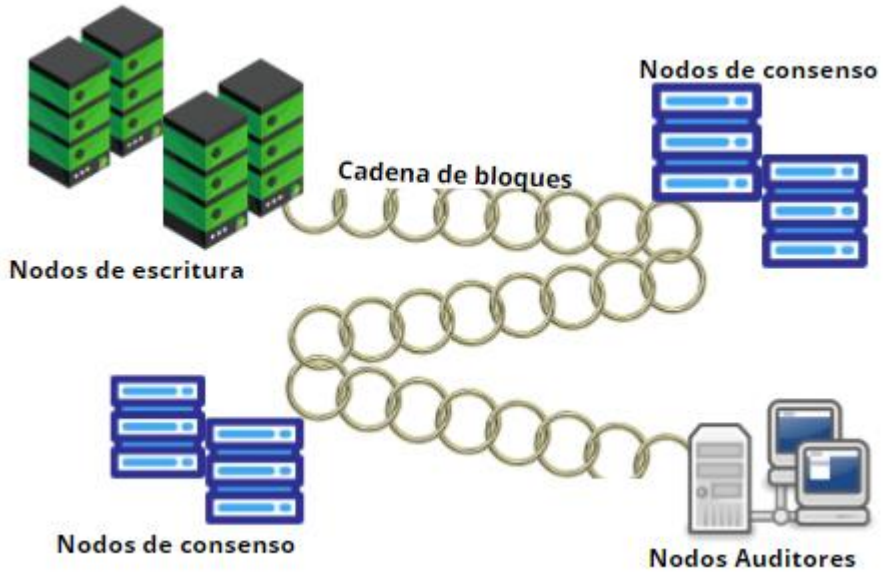
4.1.1 *Tablón de Anuncios Blockchain*

Este punto hace referencia a la cadena de bloques utilizada; consta de nodos con permisos de escritura y testigos externos reconocidos los cuales hace referencia a los nodos de consenso y por último cuenta con nodos con permisos solo de lectura. Estos últimos son nodos de auditoría los que puede utilizar cualquier persona del mundo.

Esta red cumple un papel importante en el sistema dado que proporciona un registro inmutable de todos los datos durante todas las elecciones, también funciona como sistema central de memoria y de comunicación. “El tablón de anuncios es una base

de datos de anexos en la que solamente algunos nodos autorizados pueden escribir y publicar declaraciones firmadas sobre ella" (Ágora, 2021), este proceso de enviar datos autenticados y firmados criptográficamente la hace una red más segura, confiable y auditable. En la siguiente imagen se muestra cómo funciona la primera capa.

Figura 11. Funcionamiento capa Tablón de anuncios - funcionamiento cadena de bloques.



Nota. Fuente: el autor.

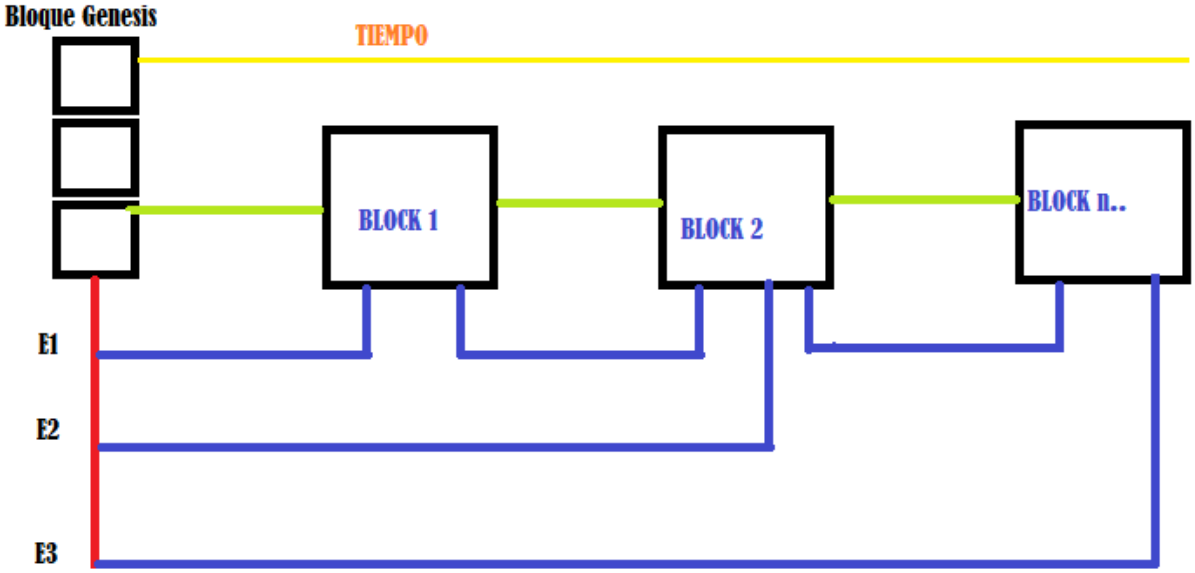
4.1.2 *Arquitectura de Skipchain*

La capa de Tablón de anuncios Blockchain funciona con base a la arquitectura Skipchain la cual brinda un mecanismo de consenso bizantino de alto rendimiento.

Es por ello que, "Skipchain es el tipo de arquitectura que se utiliza porque permite al usuario [(al votante o a cualquier persona)] navegar por la línea de tiempo de la arquitectura" (Ágora, 2021), es decir, no necesita tener todo el registro de la cadena, un usuario normal puede realizar esta verificación desde su dispositivo móvil y adicional la cadena de bloques es navegable hacia atrás sin tener conexión a internet lo que permite ser verificable por el votante.

En la siguiente imagen se muestra en forma gráfica la funcionalidad de esta arquitectura:

Figura 12. *Arquitectura Skipchain*



Nota. Fuente: el autor.

A partir de la imagen anterior, figura 10, se prosigue a explicar la arquitectura de Skipchain. Entonces, lo primero es identificar la línea de tiempo que está en color amarillo, lo que se refiere a, después del bloque génesis se van anidando los demás bloques del sistema a través del tiempo como se puede ver en la parte superior de la imagen; esta arquitectura permite la estructura de la cadena de bloques blockchain tal cual se observa en la línea verde, lo interesante y novedoso de esta es su funcionalidad como se ve en la parte inferior de la imagen. Se une por medio de enlaces que pueden ser cortos o muy largos, también es un tipo de arquitectura no lineal y bastante redundante, pero que permite la conexión y navegación a través de estos enlaces bien sea hacia adelante o hacia atrás, permitiendo que sea mucho más simple la interacción y consulta de la cadena de bloques del sistema.

Como ya se conoce las transacciones que se guardan en cada uno de los bloques tienen un número que se llama *hash*, este funciona como identificador o puntero de la transacción y del bloque, los enlaces funcionan a través de estos hashes criptográficos, mientras que para el resto del sistema son firmas colectivas de un grupo de testigos. Es válido aclarar que estos enlaces son únicamente de lectura es decir ningún usuario o entidad auditora puede realizar alguna modificación, permitiendo que sea un proceso transparente y verificable.

La arquitectura Skipchain funciona con “enlaces de corta y larga distancia” (Ágora, 2021) en un método que se llama lista convencional de enlaces, funciona en base a tres tipos de enlaces: “enlaces simples, enlaces dobles y enlaces largos” (Ágora, 2021). Como ya se había mencionado estructuralmente es redundante, pero permite un recorrido y una búsqueda mucho más eficientes.

Los bloques que conforman esta arquitectura, según la expuesta por Ágora (2021), están compuestos por:

- Hash de raíz del árbol Merkle que contiene todas las transacciones en el bloque actual.
- Hash de raíz del árbol Merkle que representa el estado actual de todo el Skipchain.
- Hash del bloque actual, actúa como puntero o identificador del bloque.
- Hash backward apuntando al bloque anterior.
- Lista de enlaces hacia adelante y hacia atrás que apuntan a diferentes bloques de la arquitectura Skipchain, para una navegación rápida dentro de la cadena.
- Lista de nodos de Cothority responsables de manejar ese bloque.

4.1.3 *Cothority - Coautoridad*

Los nodos que aseguran la etapa anterior del Tablón de anuncios, consisten en una autoridad colectiva autorizada, de ahí viene su nombre Coautoridad. Como en cualquier otra red blockchain estos nodos confirman las transacciones del sistema electoral, una transacción equivale a un voto efectivo de un usuario. Tal y como funciona en otros sistemas de blockchain cada uno de estos nodos de la red conserva una copia del registro de cada una de las transacciones y también las aprueba en bloques como método de consenso de la red, para resaltar estos nodos se supervisan entre sí para asegurarse de que el registro de transacciones en bloques se mantiene inalterado.

La plataforma consta de un conjunto de nodos de consenso que confirman las transacciones en el tablón de anuncios, las transacciones cuentan con un conjunto de datos tales como las papeletas de votación, el archivo de configuración y la prueba de consenso. De los nodos de consenso que trabajan es esta capa Coautoridad, uno de ellos es elegido rotativamente para que sea el “nodo oráculo” el cual se encarga de proponer nuevos bloques para la red así mismo recibo de papeletas y datos de los demás nodos de consenso y otra de las funciones importantes del nodo oráculo es escribir los bloques confirmados en el registro de Cotena que es otra capa la cual se explicará más adelante. El nodo oráculo y los demás nodos son operados en este caso por ÁGORA en distintas ubicaciones y también son operados por terceros involucrados e interesados en el sistema de votación.

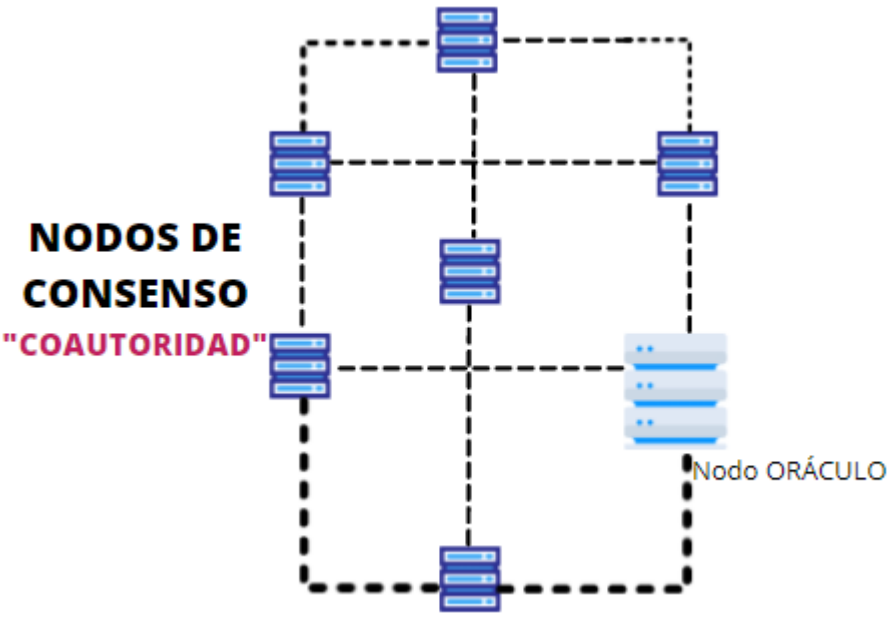
Los nodos de consenso de la capa Coautoridad tienen los siguientes propósitos:

1. Mantienen una copia de la cadena de bloques del sistema, que es la misma que se publica en la capa anterior de tablón de anuncios.
2. Recibe los votos encriptados de los votantes, actualiza los datos y verifica que el voto venga desde un usuario autorizado para que el voto sea válido.
3. Descifra los votos de los usuarios al final de las votaciones y los deja en un formato el cual se puedan contabilizar.
4. Mantiene una copia del registro de la capa de Cotena.
5. Confirma los bloques propuestos por el nodo oráculo.

El nodo oráculo el cual en términos técnicos es un servidor de la red escogido aleatoriamente en una rotación base, tiene las siguientes funciones:

1. El oráculo agrega el archivo de configuración al tablón de anuncios.
2. El oráculo crea bloques a partir de los votos autenticados y los propone a la red para su confirmación.
3. El oráculo agrega los bloques confirmados al registro y los empuja a la red blockchain Bitcoin.

Figura 13. Funcionamiento capa Coautoridad - consenso de las transacciones de la red y función del nodo Oráculo.



Nota. Fuente: autor.

4.1.4 *Segunda Capa: COTENA*

El tablón de anuncios que es la primera capa del sistema interactúa con Cotena que es la segunda capa, está inspirada en el método Catena el cual es un mecanismo de registro a pruebas de manipulaciones construido para registros que se tengan en un sistema blockchain.

En la capa de Cotena la Coautoridad gestiona un registro de solo anexo que se forma a partir de transacciones en Bitcoin**,** el sistema funciona de tal manera que el registro de toda la cadena de bloques se guarda en esta capa pero a su vez se comparte con la red Bitcoin, esto se hace con el fin de aprovechar la seguridad de los datos o como tal de la red Bitcoin, el utilizar netamente Bitcoin para una red como la que se plantea no

sería eficiente por los altos costos que maneja esta red, Cotena fue creada para aprovechar la seguridad de los datos de la cadena Bitcoin al tiempo que presenta un diseño de requisitos de almacenamiento de datos reales y costos de transacción reducidos de bitcoin.

4.1.4.1 *Cotena log:*

El registro de Cotena se basa en una lista de instantáneas del tablón de anuncios que se toman periódicamente en un tiempo definido. Los nodos de Coautoridad y la cadena de bloques de Bitcoin guardan una copia de cada actualización de registro realizada.

Para crear un registro Cotena, *Cothority* genera la dirección colectiva de Bitcoin posterior a esto firma y transmite una transacción “génesis” o de inicio tx0 a la red bitcoin. La transacción contiene la clave pública de Coautoridad como también contiene el estado de cuentas 0 y paga una cantidad inicial de bitcoin b0 a la dirección recién generada.

Para ampliar el registro o cadena de bloques. Coautoridad transmite una transacción de *Bitcoin txi* con una declaración tal que *txi* acredita una cantidad de bitcoin bi-1 de la salida de txi-1 a la dirección de Coautoridad. Este proceso crea y hace posible la producción de una cadena de transacciones.

Este registro de transacciones se puede ampliar hasta que se agoten los fondos. Para agregar más fondos al registro, las transacciones de Cotena pueden tener entradas adicionales que bloquean fondos adicionales en la salida de continuación de esa transacción. Estas entradas solo se pueden usar para agregar fondos adicionales y no se pueden usar para unir maliciosamente dos registros diferentes, ya que Cotena solo usa su primera entrada para gastar transacciones anteriores de Cotena. Los nodos que ejecutan que hacen parte de la arquitectura pueden identificar si una transacción de Cotena intenta apuntar a dos transacciones anteriores de Cotena diferentes.

Un umbral predefinido de los nodos de consenso en la Coautoridad debe aprobar cualquier registro de una nueva transacción en la cadena de bloques, esto se realiza para que un estado de cuenta sea enviado a Cotena y esto debe ser aprobado en una transacción firmada por Coautoridad, los nodos de consenso garantizan que las transacciones txi cumplan con algunas condiciones antes de ser agregadas a la cadena de bloques Bitcoin.

Las condiciones que se mencionan anteriormente son tales como:

1. La transacción txi tiene el formato de datos correcto para evitar que un miembro comprometido de Coautoridad finalice el registro con una transacción mal formada.

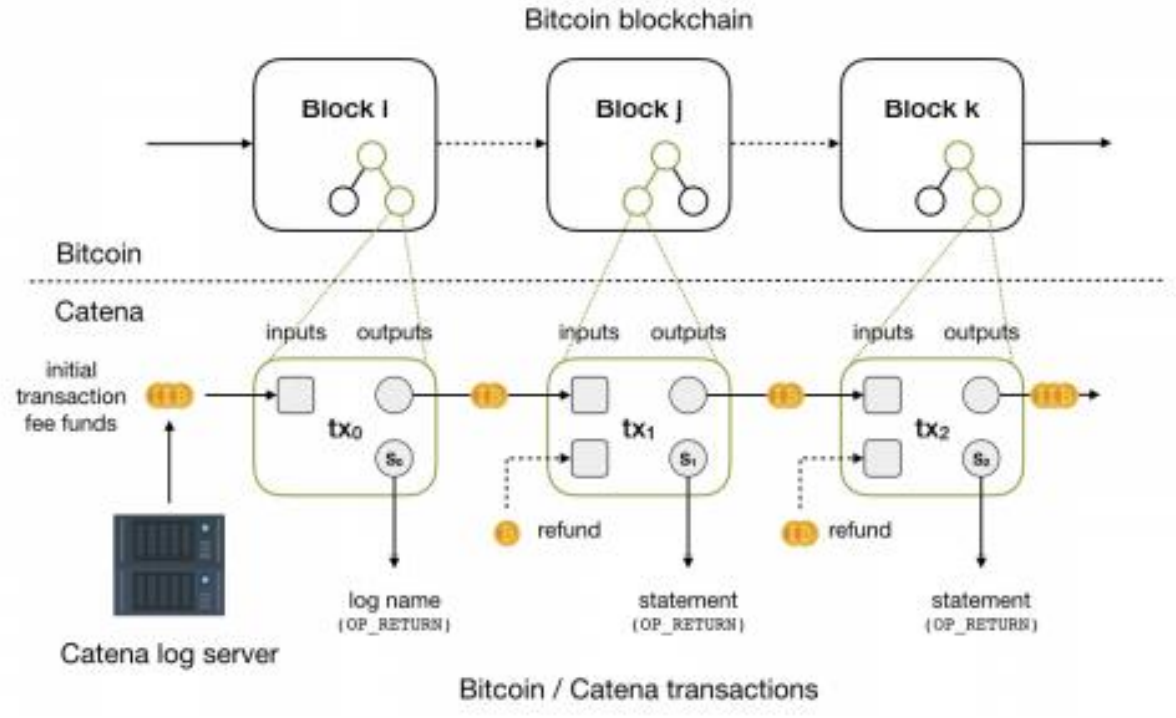
2. La declaración si está incluida en txi es compatible con la aplicación y no corrompe el estado de la aplicación.
3. La transacción txi usa la primera entrada para gastar la salida de txi-1 para evitar una fusión maliciosa de dos registros distintos.
4. La transacción txi acredita la dirección del registro y no una dirección diferente controlada por un atacante o una autoridad malintencionada que desea censurar los mensajes de los clientes.

En el inicio de esta segunda capa, Cotena incluye no sólo detalles sobre su colectivo clave pública en la transacción génesis tx0, también incluye un hash del primer Skipblock del Bulletin Board. Con esa información, un cliente puede verificar que su registro de Cotena está registrando Skipblocks de la Skipchain correcta.

Después de que se inicia un registro de Cotena por medio de una transacción génesis, la frecuencia en la actualización depende de la criptomoneda o sistema sobre el cual se esté trabajando, en el caso de Agora como trabaja con Bitcoin el tiempo de actualización en el registro es cada 10 minutos, por ende para resolver esto las transacciones tienen un registro previo el cual se realiza en el Tablón de anuncios, y posteriormente el nodo de Oracle actual envía una instantánea de su último Skipblock a Cotena. El intervalo durante el cual el tablón de anuncios envía datos a Cotena se denomina Época.

Durante la elección presidencial, cada tarjetón, transacción y otras actualizaciones se registran en el Tablón de anuncios, esto puede suceder con mucha frecuencia tal como por ejemplo una vez por minuto así mismo en intervalos menos frecuentes como una vez al día, Coautoridad realiza una actualización del registro de transacciones de Cotena con un hash del último Skipblock de la época más reciente. Dicha actualización de registro posteriormente se envía a la cadena de bloques Bitcoin para lograr una inmutabilidad y transparencia descentralizadas, este enfoque permite a Agora agregar boletas de manera escalable a una cadena de bloques descentralizada mientras logra bajos costos y latencia.

Figura 14. Transacciones Cotena



Nota. Adaptado de *Transacciones Cotena,* por Ágora, 2021, https://shallot-octopus.squarespace.com/s/Agora_Whitepaper.pdf

El Tablón de anuncios y Cotena proporcionan una configuración de cadena de bloques híbrida con permiso y sin permiso que logra una descentralización a prueba de manipulaciones con un bajo costo y un alto rendimiento de datos, cualidades con las que no cuenta una cadena de bloques Bitcoin como independiente.

Lo anterior es la base del sistema que implementa Ágora (2021) sin puntos únicos de falla, una frecuencia de actualización configurable y verificable fuera de línea.

4.1.5 *Blockchain Pública.*

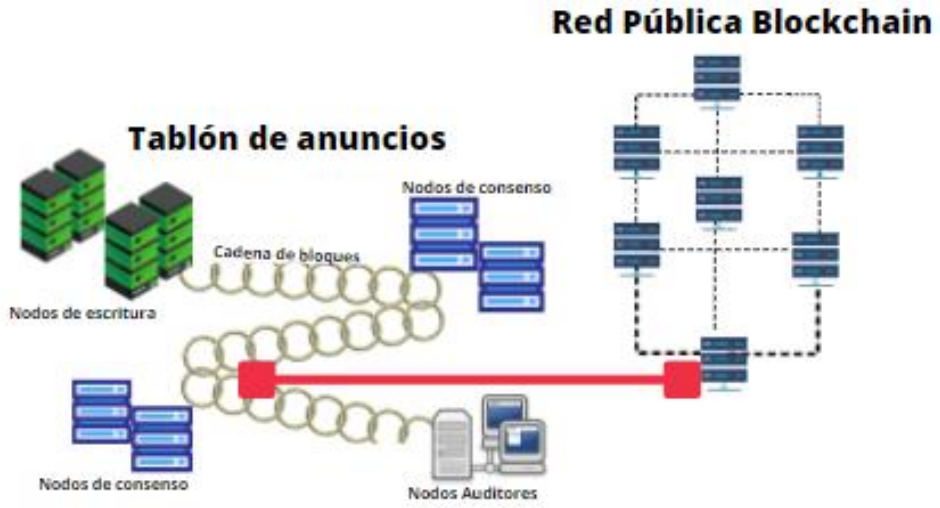
Para esta capa Agora trabaja con la red pública Bitcoin. La cadena de bloques de Bitcoin “es un libro contable digitalizado y descentralizado el cual mantiene un registro de todas las transacciones que ocurren en la red de igual a igual de Bitcoin” (Ágora, 2021). La principal novedad de esta cadena de bloques es que permite a los usuarios compartir información y almacenarla sin la necesidad de un tercero centralizado. Los datos que se almacenan en esta cadena de bloques son inmutables a los cambios lo cual hace de esta red confiable. Esta red se mantiene por nodos operados por mineros los cuales son recompensados con criptomonedas de Bitcoin.

Ágora (2021) utiliza la red blockchain de Bitcoin como parte de su arquitectura para almacenar algunos datos que el sistema requiere para ser un sistema descentralizado. La red Bitcoin es una de las redes actualmente en el mundo más grandes, por tal razón es una de las redes que se consideran más seguras y además ofrece una alta inmutabilidad de datos.

Como se había mencionado anteriormente en el apartado de Cotena, “este almacena periódicamente un hash del Skipblock más reciente en un código de operación *OP_RETURN* de transacción de Bitcoin” (Ágora, 2021), el cual permite a cualquier persona verificar que tanto el registro de Cotena y Tablón de anuncios permanecen sin cambios provocados.

Actualmente a nivel mundial existen otras redes con alto rendimiento, seguridad, y nuevos beneficios, Agora en su arquitectura trabaja con la red de Bitcoin y por eso en esta tesis se explica y se expone como lo plantean para entender el funcionamiento de esta capa en la arquitectura, lo anterior no significa que sea con la única red blockchain con la que se pueda trabajar o que un sistema como el que se plantea netamente funcione en la red Bitcoin. Para este trabajo de grado en este apartado se propone que para esta capa se utilice la red de Ethereum la cual actualmente es la más desarrollada y segura, aportando dos características fundamentales para el sistema electoral que se plantea, adicionalmente Amazon y Ethereum desarrollaron un servicio con la tecnología blockchain el cual es adaptable es su totalidad con este sistema. En el capítulo de Análisis financiero se explica y se detalla acerca de este servicio y la red Ethereum.

Figura 15. Funcionamiento capa Red Pública Blockchain - Funcionamiento y comunicación entre las redes para el manejo de la información de la cadena de bloques.



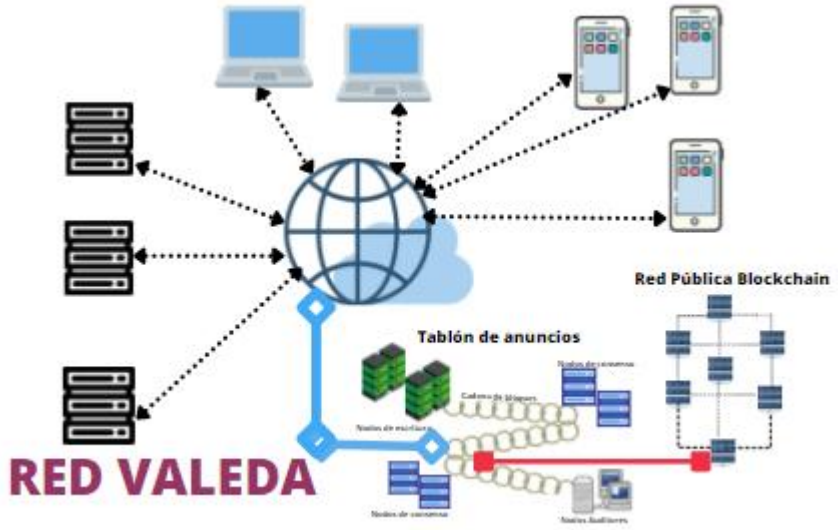
Nota. Fuente: autor.

4.1.6 *Red Valeda*

Esta capa en la arquitectura “es una red descentralizada global de nodos sin confianza la cual es la encargada de validar los resultados de las votaciones en el Tablón de anuncios” (Ágora, 2021). Esta capa cumple con una función importante, ya que es la capa encargada de proporcionar evidencia pública final de qué Coautoridad ha mantenido la autenticidad de los datos del Tablón de anuncios y comprobar públicamente que los resultados de las votaciones son correctos. “La red Valeda está compuesta por nodos ciudadanos cuyo software computa pruebas criptográficas que pertenecen a varios procesos de la arquitectura como, registro de los votos, descifrados, conteo, etc” (Ágora, 2021).

Al finalizar las elecciones y la capa Coautoridad ha calculado los votos, todos los nodos de Auditoría ciudadana de la red Valeda realizarán validaciones de los resultados.

Figura 16. Funcionamiento capa Red Valeda - Funcionamiento y consulta de auditoria por usuarios e interesados.



Nota. Fuente: autor.

4.1.7 *Votapp*

Está en la capa de aplicación dentro de la arquitectura de Ágora (2021). Funciona como una aplicación Open Surce en la cual cualquier persona puede escribir código o aplicaciones sobre Ágora para que la interacción entre esta capa y las demás sea más sencilla e intuitiva y lo mismo para el usuario final, es decir el votante. Dentro de esta capa existen tres aplicaciones principales que son Cabina de votación, Auditoría y Nodo.

Lo expuesto a continuación son categorías propuestas por el documento de Ágora (2021) para desarrollar la explicación de la aplicación Votapp:

1. *Cabina de Votación:* Esta aplicación permite al usuario final, es decir, el votante participar en la elección. Esta aplicación descarga información del archivo de configuración tal como los candidatos de las elecciones y dependiendo de las elecciones estén habilitadas otras opciones. Para este caso la información que se descarga del archivo de configuración es únicamente relacionada a los candidatos presenciales con una única opción al votar, es decir del tarjetón solo se puede seleccionar o votar por una opción o candidato, tal cual como ha sido siempre.

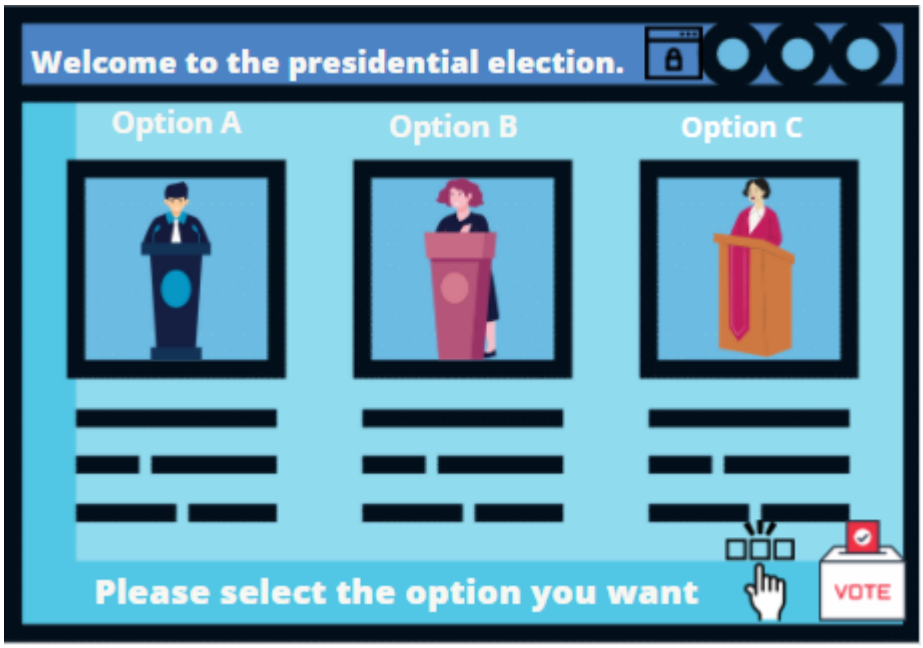
Esta boleta digital sobre la cual el votante va a dar su voto está encriptada antes de ser enviada a la capa del Tablón de anuncios, en esta aplicación de Cabina de votación le permite al usuario asegurarse de que el mecanismo de cifrado del dispositivo funcione correctamente, y también puede confirmar que su voto ha sido emitido y se ha agregado para ser contabilizado en la etapa de conteo de votos.

2. *Auditoría:* Esta aplicación permite garantizar una verificabilidad de extremo a extremo, la cual resalta una característica muy importante del sistema, la aplicación cuenta y aporta con un conjunto de herramientas las cuales son accesibles para auditar las elecciones, es válido aclarar que esta auditoría no es únicamente para el conteo de los votos, sino que por el contrario la auditoría se puede realizar sobre cada una de las capas de la arquitectura del sistema.

3. Nodo: En esta aplicación cualquier persona que quiera puede desarrollar su propio nodo en la red, el cual mantiene un historial completo de nuestro tablón de anuncios y del registro de Cotena. “Este nodo sólo puede responder a la solicitud de cualquier cliente para consultas del Tablón de anuncios” (Ágora, 2021), pero este tipo de nodos no pueden participar activamente en la red como si fuera un nodo de consenso, para que un nodo funcione como nodo de consenso debe ser evaluado por Ágora en este caso como un socio estratégico, en el caso de la red estos nodos son socios estratégicos dentro de la red desplegada y de la organización como la aprobación y consentimiento de la junta electoral, en resumidas palabras un nodo de consenso debe tener una aprobación previamente estudiada para poder serlo.

No todos los nodos son de consenso, ya que son estos los que trabajan directamente con el voto de los usuarios, resaltando nuevamente el uso de implementar una red híbrida.

Figura 17. Prototipo del home de la aplicación en donde los usuarios votaran.



Nota. Fuente: autor.

4.2 Proceso de Votación

Las elecciones con un sistema, así como el que plantea Ágora (2021) y como el que se busca, teniendo en cuenta, la escalabilidad de este proyecto. Es la apropiada. El diseño de esta red blockchain para votaciones electorales garantiza que se cumplan características y requisitos tecnológicos importantes para mantener una elección confiable, verificable, con privacidad, descentralizada y escalable de extremo a extremo, tal como afirma la empresa Ágora.

Esto permite que unas elecciones electorales a nivel nacional sean posibles permitiendo al gobierno y organizaciones celebrar elecciones en una plataforma digital totalmente verificable.

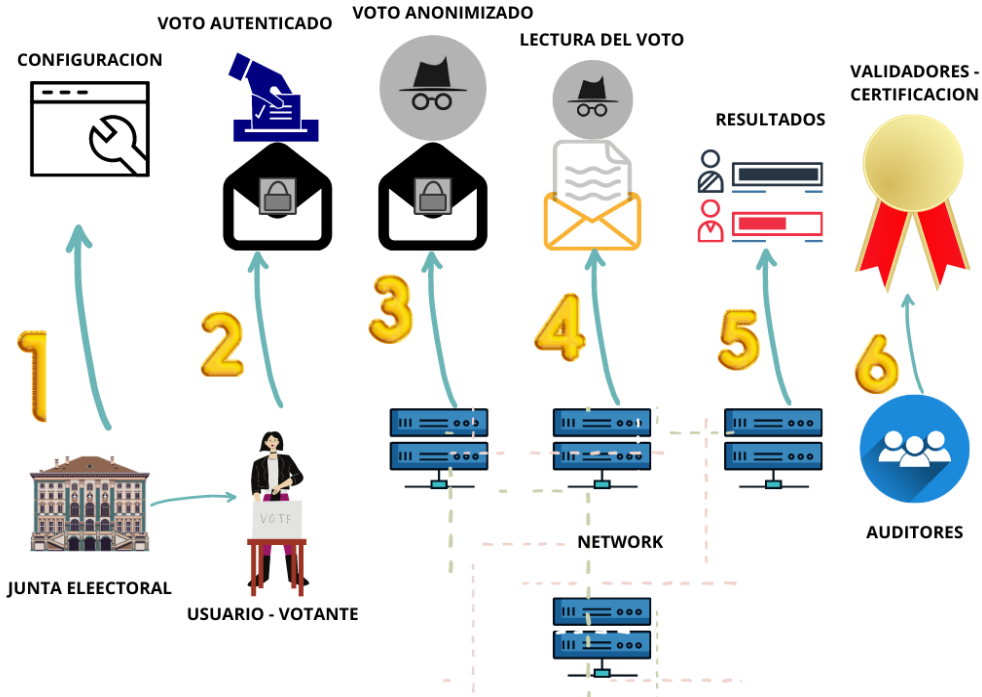
En el siguiente apartado se explicará cada una de las etapas desde el inicio hasta el final de las elecciones, es válido aclarar que no se trata de una explicación técnica pero que si ayuda a entender cómo cada una de las capas del diseño interactúan con las distintas capas explicadas anteriormente.

4.2.1 *Proceso de Votación:*

El proceso de votación planteado tiene seis pasos sobre los cuales se desarrolla. Estos se encuentran expuestos textualmente en el informe de Ágora (2021) y se presentarán a continuación:

> “Estos pasos ofrecen una solución de votación criptográficamente verificable en la cual la confianza depositada por el usuario será altamente gratificada.
>
> Estos son:
>
> 1. *Configuración:* La junta electoral junto con los administradores de la misma crean un nuevo evento de elecciones presidenciales para este caso.
> 2. *Fundición:* Los votantes emiten sus votos cifrados a la red
> 3. *Anonimización:* La red anonimiza todas las boletas electorales para que su rastreo no sea posible.
> 4. *Descifrado:* La red descifra las papeletas anónimas.
> 5. *Conteo:* Se cuentan los votos.
> 6. *Revisión:* Los auditores netos de las elecciones así mismo las auditorías públicas de los observadores publican revisiones que confirman la validez de los resultados de las elecciones.” (p.26)

Figura 18. *Pasos Proceso de Votación*



Nota. Fuente: el autor.

Este proceso se compone por varios pasos o procesos que juntos hacen que el funcionamiento de las elecciones con el modelo planteado sea totalmente funcional, a continuación, se detalla cada uno de los seis pasos anteriormente mencionados en la imagen.

4.2.1.1 *Configuración:*

Para la configuración de las elecciones los administradores crean un evento el cual contiene:

> "Un archivo de configuración el cual incluye todas las reglas y parámetros específicos del evento, entre algunos de estos pueden las personas habilitadas para votar, identidades de los funcionarios responsables y de los votantes, fecha y hora de inicio y finalización, candidatos a elegir" (Ágora, 2021, p.27),

Teniendo en cuenta que, el tipo de elección para este caso, en el marco del proyecto, serán presidenciales, entre otros, a continuación, vamos a profundizar brevemente en los más importantes:

- *Funcionarios electorales:* En el archivo de configuración se tendrán "valores que incluyen los nombres y claves públicas de los funcionarios electorales" (Ágora, 2021). Para una mayor verificabilidad y descentralizar la confianza puede ser una misma clave pública y única la cual se genera y se distribuye a través de un protocolo.
- *Tipo de elección:* En el archivo de configuración se tendrá un valor el cual será el que determine qué tipo de elección será, en este valor se configura para estas elecciones en especial un único voto intransferible y que únicamente puede seleccionar a un candidato, es decir un voto por votante para elegir un candidato.
- *Fecha y horas:* Estos valores: Estos valores que se configuran determinan el marco de tiempo de durabilidad en que los votantes pueden emitir sus votos.
- *Votantes:* Esta lista contiene todos los votantes que realizaron el registro previo y los cuales están en la lista de votantes autorizados para emitir su voto.
- *Candidatos:* Esta lista tiene configurado los valores sobre los cuales los votantes deben elegir.
- *Lista de observadores o auditores:* Para estas elecciones este valor es importante debido a que entre más verificables sean las elecciones será mucho mejor, los funcionarios electorales pueden asignar observadores o auditores los cuales se encargaran de verificar la transparencia del evento electoral, para esto se deben configurar los valores de identidades y claves públicas asociadas.

"Una vez los parámetros electorales se encuentren configurados en el archivo de configuración, los funcionarios generan un identificador único criptográfico para el archivo

a través de una función hash criptográfica que puede actuar como el ID de las elecciones" (Ágora, 2021).

Este archivo se almacena y publica en la capa de Tablón de anuncios y "estará disponible para la validación pública, después de las validaciones de interesados y público aprobando la transparencia del mismo" (Ágora, 2021), el sistema estará listo para que los usuarios o votantes puedan emitir los votos.

4.2.1.2 *Casting*

En este paso el usuario se dispone a emitir su voto para lo cual "puede utilizar su dispositivo móvil y realizarlo pero se entiende que para temas de confianza del usuario y brindar un sistema de ayuda en cuanto a la gestión de que el usuario o votante pueda emitir su voto" (Ágora, 2021), se dispondrán de cabinas tecnológicas con este fin, en las sedes de votación estarán los funcionarios electorales los cuales estarán en la capacidad de realizar este acompañamiento y asesoramiento para que las personas puedan emitir su voto sin mayor complicaciones.

Independientemente del dispositivo que utilice el votante obtiene los parámetros electorales del Tablón de anuncios y permite al usuario completar una boleta de votación. El usuario posteriormente selecciona una de las opciones que le presenta el Tablón de anuncios y después de elegir el usuario puede emitir su voto.

Seguido a esto y según lo planificado por el trabajo de Ágora (2021) se afirma que:

> "Una vez el usuario ha emitido su voto, el software de votación lo cifra con la clave pública colectiva de Cothority, que son los nodos de consenso distribuidos de la red. El software utiliza el criptosistema de umbral ElGamal para el cifrado, esto es un tipo de criptografía, es uno de los mejores sistemas de encriptación" (p.29).

Para comprobar que el sistema de encriptación está funcionando correctamente lo que se realiza es realizar un test cuantas veces se quiera a un dispositivo de prueba, es decir un usuario que desee validar que el sistema de encriptación está funcionando bien y que su voto no es revelado puede pedir esta prueba y emitir un voto al dispositivo de prueba y verificar desde este mismo que el voto emitido se encuentra encriptado y que el sistema es seguro.

Una vez que se confirma que el cifrado del dispositivo de votación funciona correctamente, el votante emite su voto cifrado colocándolo en el Tablón de anuncios y firmando la transacción con sus credenciales de identidad digital. "Posterior a esto uno de los nodos de Cothority recibe el voto encriptado y lo auténtica" (Ágora, 2021). Los votos autenticados se incluyen en el Tablón de Anuncios en el próximo Skipblock.

4.2.1.3 *Anonimización*

Una vez finalizan las votaciones el sistema ejecuta todos los votos a través de una red de mezcla para anonimizar las boletas encriptadas emitidas en el Tablón de anuncios.

"Una red de mezcla es un conjunto de servidores que vuelven a cifrar secuencialmente un conjunto de datos dado varias veces, donde la corrección de cada nuevo cifrado está atestiguado por pruebas de conocimiento cero" (Ágora, 2021). Estas pruebas de corrección se publican en el tablón de anuncios para permitir la auditabilidad de este proceso. Se recomienda para un sistema de esta magnitud implementar una red de mezcla basada en *Neff-shuffle*.

Cuando los votos se envían a través de la red de mezcla, cada nodo de mezcla procesa la lista completa de votos encriptados y genera una nueva lista de votos anónimos junto con pruebas de conocimiento cero.

4.2.1.4 *Descifrado*

Para realizar el recuento de los votos "los nodos de Cothority descifran los votos y los publican con pruebas de corrección de descifrado en el Tablón de anuncios" (Ágora, 2021).

Seguido a esto y según lo planificado por el trabajo de Ágora (2021) se afirma que:

> "Al comienzo de este proceso los nodos de Cothority verifican que las pruebas de conocimiento realizadas en la fase anterior de Anonimización sean correctas, de ser así, los nodos comienzan a descifrar colectivamente las papeletas anónimas. En este proceso, cada nodo de Cothority descifrar parcialmente cada uno de los votos anonimizados y genera una prueba de conocimiento cero para cada descifrado, lo que da fe de la corrección del descifrado parcial. Una vez finalizado este proceso los nodos de Cothority publican los resultados en el Tablón de anuncios" (p.30).

Luego, la verificación de las pruebas de conocimiento cero de los votos parcialmente descifrados pueden realizarse por parte de los administradores del sistema electoral sean correctas, siempre que un umbral suficientemente alto de ellos sea válido, "los administradores pueden usar los votos debidamente descifrados parcialmente para recuperar los votos anónimos originales sin ningún formato" (Ágora, 2021), es decir, en texto plano. Estos votos se envían al Tablón de anuncios en donde se pueden contar.

4.2.1.5 *Hablar*

Después de la fase anterior de descifrado todos los nodos cuentan los votos descifrados y publican los resultados finales en el Tablón de anuncios.

"Los administradores electorales o un tercero que supervise las elecciones pueden contar los votos sin formato publicados en el Tablón de anuncios en la fase anterior" (Ágora, 2021). El departamento encargado de la junta electoral designado para el conteo de votos publica los resultados firmados en el Tablón de anuncios, momento en el que los auditores pueden comprobar la validez del resultado antes de que considere definitivo un resultado de los mismos.

4.2.1.6 *Auditoría*

"La capacidad para auditar cada uno de los boletos digitales del voto emitido por cada usuario o votante es uno de los principales beneficios de utilizar este sistema electoral" (Ágora, 2021). El diseño planteado de esta red está basado en la tecnología Blockchain la cual engrana perfectamente en la arquitectura de las capas Tablón de anuncios, Cotena registro y Valeda, siendo estas capas de la arquitectura elementos importantes del sistema que permiten mejorar las capacidades de auditoría, siendo un sistema transparente y confiable, estas capacidades pueden ser utilizadas por observadores o auditores de la elección y validar la data en la capa Tablón de anuncios.

Recuérdese que "los nodos auditores pueden ser ciudadanos, administradores o funcionarios electorales, los mismos usuarios o votantes o cualquier tercero interesado en la verificabilidad de las votaciones" (Ágora, 2021). Una vez se realice la validación de las elecciones de parte de los funcionarios de la junta electoral designados para realizar la auditoría pueden dar fe de los resultados y publicar un certificado firmado en el tablón de anuncios afirmando el correcto funcionamiento y transparencia del mismo.

"Para permitir la verificabilidad de un extremo a otro para los observadores, todos los pasos intermedios del proceso electoral son verificables por terceros y se publican en el Tablón de anuncios" (Ágora, 2021). Un observador o auditor puede realizar las siguientes verificaciones:

Entonces y según lo planteado por el trabajo de Ágora (2021) se afirma que:

- *"Configuración:* Los nodos de auditoría confirman que los parámetros sean los correctos, algunos de estos observadores pueden tener derechos adicionales otorgados por algún administrador o funcionario de la junta electoral que les permite verificar la relación entre las credenciales privadas de los votantes y la información pública en el Tablón de anuncios.
- *Casting:* Los nodos de auditoría confirman que cada voto encriptado publicado en el Tablón de anuncios esté correctamente vinculado a uno de los usuarios del sistema, así mismo pueden corroborar que el cifrado o encriptación del voto esté funcionando correctamente y que este se encuentre en el formato adecuado.

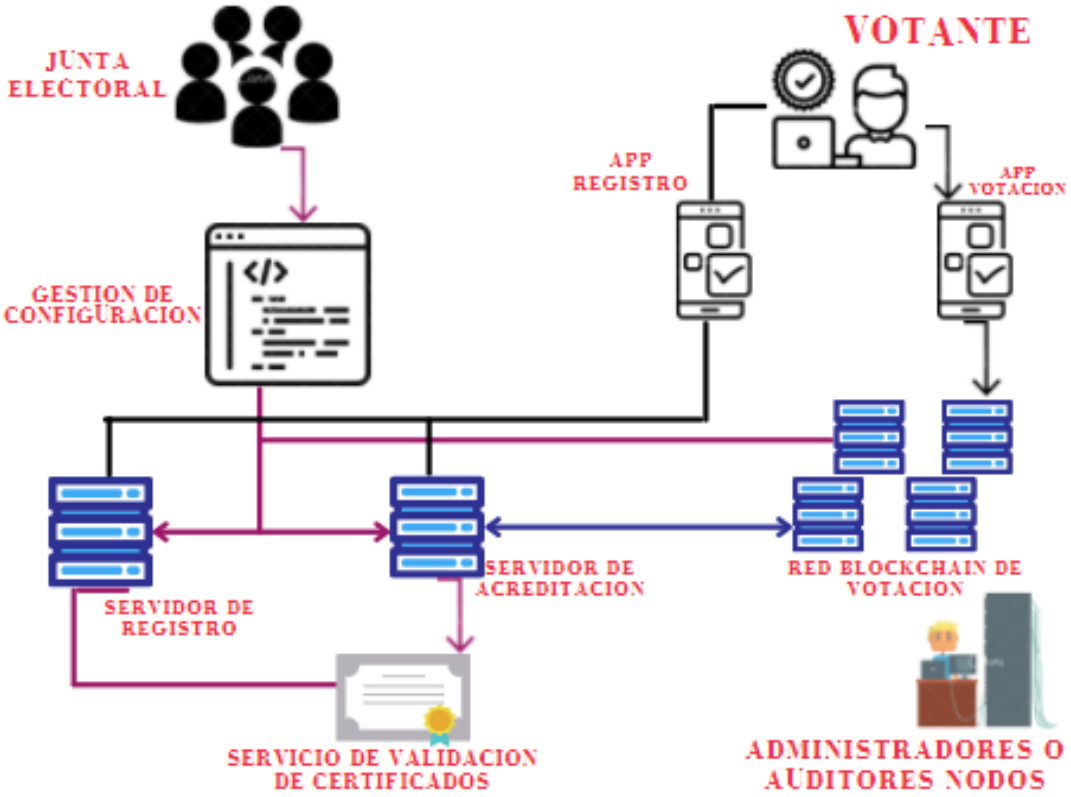
- *Anonimización:* Los nodos de auditoría pueden verificar que cada uno de los votos encriptados en el Tablón de anuncios se ha barajado y anonimizado correctamente. Esta verificación incluye todas las pruebas de conocimiento cero.
- *Descifrado:* Los nodos de auditoría verifican que todos los votos descifrados son correctos con respecto a las correspondientes pruebas de descifrado de conocimiento cero, y que los votos en texto plano se reconstruyan correctamente a partir de los votos parcialmente cifrados.
- *Contando:* Los nodos de auditoría realizan la validación y confirman que los resultados de las elecciones se computan correctamente a partir de los votos en texto plano" (p.31).

Si el proceso es totalmente confirmado y debidamente auditado con éxito el observador firma un certificado final con la clave privada del observador, administrador o funcionario de la junta electoral. "Esta firma final puede tener un valor especial agregado como firma o certificado especial para el cierre de las votaciones" (Ágora, 2021) y toma un mayor valor cuando este funcionario es parte imparcial y de confianza ampliamente reconocida.

5. Financiero y Costo de la Solución

A continuación, se describirán cada uno de los actores principales que componen y hacen parte de este sistema electoral (personas, los sistemas y las entidades con las que interactúan). Esto permitirá tener un panorama y contextualizar el sistema en general y entender cómo se relacionan los actores de la solución con los diferentes elementos del mismo.

Figura 19. *Contexto General de la Solución*



Nota. Inspirada del texto guía. Fuente: el autor.

De la imagen anterior, figura 13, se obtiene la solución del sistema planteado de una forma general y contextualizada, en cuanto a la parte de infraestructura de los servidores y servicios se tiene el servidor de registro y el servidor de acreditación; estos servidores pueden estar en uno solo y no es tan necesaria su separación, pero por seguridad del sistema se plantea de esta forma ya que así mismo que se ha nombrado anteriormente en donde el registro se hace en un momento y la habilitación de las credenciales del voto en el momento de la votación. También, se realiza la separación a nivel físico, de esta manera se dificulta la trazabilidad y correlación entre las solicitudes de

registro y acreditación. Adicionalmente, se tienen los servidores desplegados que funcionan como nodos de votación de la red blockchain.

5.1 Servicio de Registro:

El servicio de registro es en donde se gestiona todo lo relacionado al registro de los votantes, este servicio cuenta con varios componentes principales para su funcionamiento, estos componentes tienen sentido de gestión, es decir un proceso que hace parte para el correcto funcionamiento del servicio como así mismo componentes técnicos tales como las interfaces que de igual manera son parte fundamental del servicio ya que son la interacción del usuario con el servicio, a continuación se explicara cada uno de ellos:

- Gestión de Usuarios: Este componente es el que se encarga de la seguridad en cuanto a las autorizaciones que debe tener un cliente o usuario para acceder y hacer uso de las funcionalidades de la aplicación.
- Gestión de errores: Este componente es el que se encargará de los errores que se puedan dar durante el registro de un usuario.
- Gestión de Configuración: Este componente se encarga de la configuración del servicio para el registro de los usuarios, es decir grupo de votantes, requisitos de registro, etc.
- Gestión de Credenciales de firma: Este componente se encargará de almacenar las credenciales de firma que se utilizaran para los registros de cada uno de los usuarios, es decir contiene una firma por cada grupo de votantes, este componente es uno de los que requiere mayor seguridad.
- Gestión de votantes: Este componente se encarga del flujo del registro de los usuarios.
- Validación de votantes: Este componente es el encargado de realizar la validación del usuario para el registro es decir cumplimiento de los requisitos, no haberse registrado anteriormente, etc.
- Firma de solicitud: Este componente trabaja directamente con el componente de gestión de credenciales, y es el encargado de realizar la firma digital sobre la solicitud del votante.
- Mantenimiento de registro de votantes: Este componente es el encargado de mantener actualizado el registro de usuarios o votantes según las solicitudes que se realicen.
- Interfaz petición de registro: Es la interfaz con la que el usuario interactúa para realizar la petición de registro.
- Interfaz de notificación del registro: Es la interfaz mediante la cual el sistema recibe la notificación del registro del votante telemático.
- Interfaz de conexión con entidades validadoras: Es la interfaz del sistema con las entidades validadoras de los certificados de los usuarios o

votantes con las cuales se identifican. Este caso sería el documento de identidad o cédula o un certificado por parte de la registraduría el cual apruebe que la persona está habilitada para votar.

5.2 Servicio de Acreditación:

Este servicio es el que acredita al votante para realizar el voto, es decir, es el que carga las credenciales de voto en el momento en que el votante se dispone a realizar su elección. Recordemos que para el planteamiento de esta solución se tiene separado el servicio de registro, que se explicó anteriormente, y el de acreditación que se reitera es en el momento en que el votante se dispone a dar su voto. A continuación, se explicarán los componentes que hacen parte de este servicio:

- Gestión de Usuarios: Este componente es el que se encarga de la seguridad en cuanto a las autorizaciones que debe tener un cliente o usuario para acceder y hacer uso de las funcionalidades de la aplicación.
- Gestión de errores: Este componente es el que se encargará de los errores que se puedan dar durante la acreditación de un usuario.
- Gestión de Configuración: Este componente se encarga de la configuración del servicio para el registro de los usuarios, es decir grupo de votantes, requisitos de registro, etc.
- Gestión de Credenciales de firma: Este componente se encargará de almacenar las credenciales de firma que se utilizaran para los registros de cada uno de los usuarios, es decir contiene una firma por cada grupo de votantes, este componente es uno de los que requiere mayor seguridad.
- Gestión de peticiones: Este componente es el encargado de recibir la petición del usuario de las credenciales para votar y será quien gestione la funcionalidad principal del flujo.
- Validación de firma: Este componente es el encargado de realizar las validaciones de la firma recibida en la acreditación, se encargará de validar que es la misma firma digital dada por el sistema de registro, y que pertenece al grupo de votantes correcto.
- Generación de transacciones: Será el componente encargado de generar las transacciones es decir será quien se encargue de transferir el voto a la dirección previamente acreditada.
- Mantenimiento de registro de direcciones: Este componente se encarga de mantener actualizadas las direcciones que se utilizaran en el componente anterior de transacciones.
- Interfaz de petición de acreditación: Es la interfaz que le permite al usuario acreditar la dirección de voto.

- Interfaz conexión con nodos de red blockchain: Es la interfaz del sistema que se comunica con los nodos de la red de votación para realizar el envío de las transacciones con los votos acreditados.
- Interfaz con entidades validadoras: Es la interfaz del sistema con las entidades validadoras de los certificados que se utilizan durante la acreditación.

5.3 Nodo de Votación:

Los nodos de votación serán los encargados de gestionar toda la fase de acreditación de los usuarios, a continuación, se detallarán los componentes funcionales del servicio de acreditación:

- *Gestión de usuarios:* Este componente se encarga de la seguridad y autorizaciones para acceder a las funciones de la aplicación.
- *Gestión de errores:* Este componente es el que se encargará de los errores que se puedan dar durante el proceso.
- *Gestión de configuración:* Este componente es el encargado en cuanto a la configuración de la votación es decir direcciones de votaciones, grupos de votación asignados, reglas de votación, etc.
- *Gestión de transacciones:* Este componente será el encargado de la recepción de peticiones de transacciones y también se encargará de la gestión de las mismas. Así mismo se encarga de la actualización de la tabla de transacciones pendientes por realizar.
- *Validación de transacciones:* Este componente realizará las validaciones las validaciones de las transacciones que se reciben, se encarga de validar que la transacción es correcta es decir que no utiliza más votos de los asignados y que cumple con las reglas estandarizadas.
- *Generación de bloques:* Este componente será el encargado de agrupar las transacciones para la generación de nuevos bloques.
- *Validación de bloques:* Este componente será el encargado de validar cada uno de los bloques y en sí toda la cadena de bloques, es quien se encarga de mantener la cadena actualizada al recibir nuevos bloques de otro nodo.
- *Propagación de bloques:* Este componente es el encargado de gestionar la propagación de los bloques entre los nodos, este componente es importante en el consenso del blockchain.
- *Descifrado de la cadena:* Este componente es el encargado de descifrar el contenido de las transacciones de la cadena de bloques una vez se tenga la clave privada para realizar el proceso.
- *Recuento de resultados:* Este componente se encarga de recorrer la cadena de bloques y las transacciones leyendo los votos emitidos y contabilizando

el resultado. Realiza este proceso según las reglas configuradas en el componente de configuración.

- *Interfaz de petición de transacción:* Es la interfaz desde la cual el nodo recibirá la notificación de inserción en la cadena de una nueva transacción.
- *Interfaz petición de resultados:* Es la interfaz desde la cual el sistema recibe la notificación de los resultados de las votaciones.
- *Interfaz de conexión con los nodos de la red blockchain:* Es la interfaz mediante la cual el sistema se conecta con los nodos de la red de votación para el envío de las transacciones o votos acreditados.

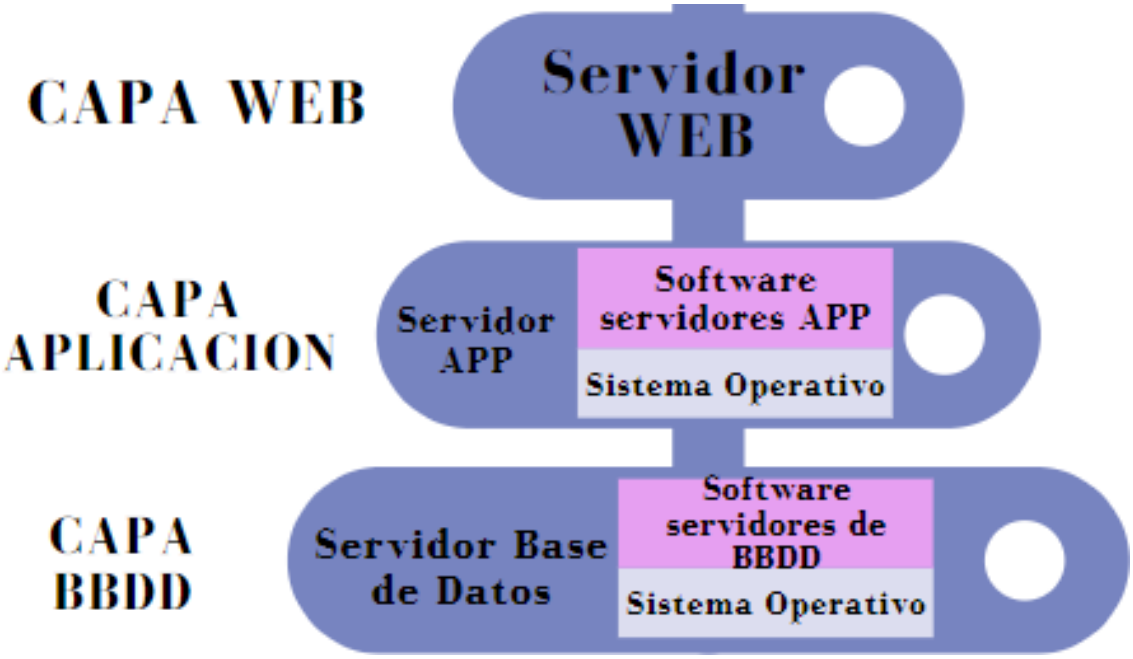
5.4 Implementación de la Arquitectura

Según la solución propuesta para este proyecto se necesitan dos tipos de implementación:

- *Aplicación web:* Será quien soporte los servicios que se ofrecen a los usuarios es decir la interacción entre el sistema y los usuarios, para este proyecto el usuario hace uso de las aplicaciones web en el momento del registro y acreditación, desde el planteamiento inicial se han mantenido estos dos servicios por aparte a lo cual se recomienda que las aplicaciones web para estos dos servicios también sean diferentes. La aplicación de acreditación es la misma de votación, recordemos que el usuario después de un registro efectivo el día de la votación cumpliendo con las especificaciones anteriores recibe la acreditación y las credenciales de voto para que pueda tomar su elección, por tal razón no se cuenta con una aplicación diferente para votar, sino que es la misma aplicación de acreditación la cual tendrá un segmento para que los usuarios voten.
- *Nodo blockchain*: Prestará los servicios de nodo de votación es la parte backend del sistema para que se entienda de una mejor forma, para este caso existirán tantas instancias como nodos quieran incorporarse, es donde se comunicara y se gestionará todo el proceso de las elecciones por medio de la red blockchain.

Para el desarrollo de esta implementación se propone que se realice mediante una arquitectura de tres capas, las cuales se explican en la figura 14 que sigue a continuación:

Figura 20. *Capas de Arquitectura*



Nota. Inspirada del texto guía. Fuente: el autor.

En la imagen anterior, figura 14, se describen las tres capas de la arquitectura que se plantea para el funcionamiento de la solución. La primera capa es la capa web, la cual es la capa de presentación y acceso web, la interacción del usuario con el sistema se hará a través de esta primera capa. La segunda, es la de aplicación y es la capa donde residen las aplicaciones que soportan los componentes funcionales de la solución. Finalmente, la tercera capa es la capa de base de datos y es la capa con los componentes de base de datos y almacenamiento. Esta arquitectura es la que se plantea para los servicios web que tendrá el sistema para los servicios de registro y acreditación que recordemos es la misma de votación y que comprende los nodos de votación de la red, es decir es en donde se reciben o recepcionan los votos de los usuarios claramente de forma telemática.

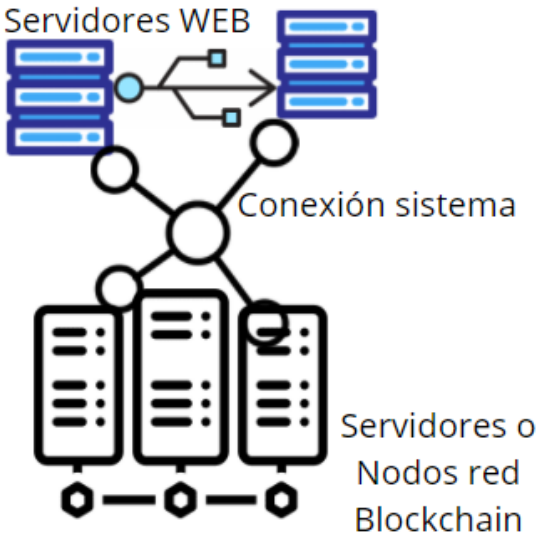
5.5 Solución General del Sistema

La solución general del sistema se realizará de dos formas las cuales ya se han explicado cada una por aparte en este proyecto. Una es toda la red blockchain, la cual será la encargada de toda la gestión de los votos de los usuarios a nivel nacional, esta red funciona y se basa netamente en la tecnología Blockchain y lo más importante es que el modelo planteado tomado de la empresa ÁGORA tiene gran escalabilidad la cual es propicia para este proyecto. Y dos es la parte web donde se desarrollarán los servicios que tendrán la interacción con el usuario, y va a ser la comunicación directa con la red

blockchain del sistema, estas dos partes se tendrán que unir y engranar perfectamente para que la solución sea exitosa.

La arquitectura planteada en general para toda la solución del sistema va a ser una red híbrida, es decir, entre privada y pública y acá se dirá el porqué: va a ser privada y centralizada en cuanto a los servicios web con los que interactúa el usuario, pero es pública y descentralizada en cuanto al funcionamiento de la red blockchain de las votaciones. En la siguiente imagen, figura 15, se explica lo anterior.

Figura 21. *Distribución General del Sistema*



Nota. Fuente: el autor.

Toda esta solución requiere de un alto poder de trabajo computacional, para lo cual se plantea alojarla y que funcione con la tecnología “Cloud”, esta tecnología actualmente es una de las más demandadas por su gran capacidad de almacenamiento, seguridad y escalabilidad de proyectos, lo cual para este red de votaciones encaja perfectamente, además que existen muchas compañías importantes a nivel mundial como: “IBM Blockchain Cloud Services, Ethereum Blockchain as a Service de Microsoft y Amazon Managed Blockchain” (Morales, 2021). Lo cual da un respaldo total y apoyo a la tecnología y a la solución planteada para este proyecto.

La solución y con fin de poder dar unos valores aproximados a los costes de la solución en general será enfocada en el servicio que ofrece Amazon, esta decisión también se toma porque la solución Amazon Managed Blockchain trabaja directamente con la red Ethereum de blockchain la cual es la más confiable, grande, segura y con mayor desarrollo en la actualidad. A continuación, se explicará más a fondo.

El 30 de abril de 2019, AWS anunció la disponibilidad de su solución Amazon Managed Blockchain como un nuevo servicio web en la nube de Amazon. “Esta proporciona una solución para tener un libro mayor (ledger) inmutable y verificable entre múltiples partes para realizar transacciones sin una autoridad central confiable” (Morales, 2021). Esta solución facilita la configuración, implementación y administración de redes blockchain escalables “utilizando soluciones de código abierto como Hyperledger Fabric y Ethereum” (Morales, 2021).

Una vez desplegada la red, el control sobre la misma pasa a manos de los interesados de la solución del sistema. Además, “la arquitectura sobre la que se implantan estas redes sigue la arquitectura de un sistema distribuido, desplegando cada uno de los nodos de la red sobre distintos servidores” (Piedra, 2018). Por otra parte, el desarrollo y despliegue de los *Smart Contracts* queda a disposición de la configuración realizada por la junta electoral configurando las reglas para el desarrollo de las elecciones, por lo que es la misma entidad y todos los interesados en el proyecto quienes configuren las reglas estipuladas y la lógica que se ejecutará en la cadena de bloques.

Para el diseño de la red blockchain planteada en este proyecto se utilizarán los servicios de Amazon *Managmend* por su gran capacidad de escalabilidad, costos y respaldo tecnológico que esta compañía a nivel mundial ofrece, antes de mostrar los valores comerciales, profundizaremos un poco más en el servicio que AWS ofrece.

El precio de la solución que se dará más adelante es para un servicio de Amazon *Managed Blockchain* para Ethereum, los precios de nodo de pares bajo demanda Amazon *Managed Blockchain* elimina la sobrecarga requerida para aprovisionar hardware manualmente y puede escalar fácilmente la infraestructura hacia arriba o hacia abajo para satisfacer las demandas de la aplicación. Con los costos de los nodos de pares de Amazon Managed Blockchain, se paga por los nodos que crea. Se paga por segundo, con un mínimo de un minuto.

5.5.1 *Almacenamiento de nodos pares*

Los nodos pares de Ethereum almacenan un historial de todas las transacciones en la red. Una de las ventajas más importantes de Amazon Managed Blockchain, el almacenamiento de sus nodos pares se adapta automáticamente a las necesidades de escalabilidad del proyecto. El almacenamiento del nodo del mismo nivel se cobra en incrementos de GB por mes.

5.6 Forma de Obtener los Costos del Diseño de la Red Blockchain

Para obtener un costo aproximado de la red Blockchain y como tal para este método de votación que se plantea en este trabajo se tendrán varios aspectos importantes como: la información que nos brinda AWS con su servicio Amazon Managed

Blockchain que como se ha venido explicando es en donde se monte la red, nodos o servidores de la red blockchain, de información de AWS se obtienen unos costos que se manejan actualmente los cuales dependen de aspectos tales como capacidad de servidores o nodo y cantidad de nodos. Esto se obtiene con la cantidad total de personas habilitadas para votar a nivel nacional y con la cantidad de peticiones (Request) que realiza cada persona al sufragar. Los detalles de estos datos se obtienen a continuación.

Tomando de referencia el ejemplo que da la página oficial de AWS, (Amazon, 2021), se deben obtener datos específicos para dar un valor aproximado del costo de este modelo de votación. Los detalles de estos datos se obtienen a continuación:

5.6.1 *Censo Electoral a Nivel Nacional*

Lo primero que se debe conocer es la cantidad total de los votantes en todo el territorio colombiano, esta información se obtiene directamente de la Registraduría Nacional de Colombia (2021) y se observa en la tabla que se muestra a continuación:

Tabla 2. *Potencial Electoral por Departamento en Colombia*

DEPARTAMENTO	**HOMBRES**	**MUJERES**	**MESAS**	**PUESTOS**	**TOTAL**
AMAZONAS	26.548	25.034	162	25	51.582
ANTIOQUIA	2.409.116	2.609.894	14.750	1.160	5.019.010
ARAUCA	108.560	103.219	638	68	211.779
ATLANTICO	959.593	1.042.103	5.898	298	2.001.696
BOGOTA D.C.	2.824.103	3.202.670	17.190	901	6.026.773
BOLIVAR	834.830	850.158	5.143	607	1.684.988
BOYACA	489.665	501.648	3.038	395	991.313
CALDAS	395.265	414.475	2.432	307	809.740
CAQUETA	156.462	151.509	929	135	307.971
CASANARE	152.488	149.113	966	164	301.601
CAUCA	496.468	516.189	3.246	785	1.012.657
CESAR	429.329	436.039	2.617	289	865.368
CHOCO	162.183	167.066	1.174	419	329.249
CONSULADOS	396.964	463.541	1.373	250	860.505

CORDOBA	654.534	659.991	3.981	518	1.314.525
CUNDINAMARCA	990.618	1.030.414	5.995	503	2.021.032
GUAINIA	16.416	14.772	101	24	31.188
GUAVIARE	34.916	27.552	199	38	62.468
HUILA	434.703	442.839	2.602	233	877.542
LA GUAJIRA	312.119	330.727	1.939	194	642.846
MAGDALENA	507.063	509.738	3.069	358	1.016.801
META	385.977	385.102	2.327	267	771.079
NARIŃO	571.341	602.140	3.817	903	1.173.481
NORTE DE SANTANDER	630.596	664.036	3.871	430	1.294.632
PUTUMAYO	121.022	117.531	740	100	238.553
QUINDIO	234.118	252.359	1.438	128	486.477
RISARALDA	395.231	431.241	2.420	199	826.472
SAN ANDRES	24.577	26.537	146	8	51.114
SANTANDER	864.352	904.970	5.534	777	1.769.322
SUCRE	366.353	360.906	2.254	400	727.259
TOLIMA	549.461	559.386	3.358	461	1.108.847
VALLE	1.710.271	1.948.081	10.858	1.082	3.658.352
VAUPES	12.638	10.589	77	25	23.227
VICHADA	28.426	24.106	169	53	52.532

Nota. Tomada de *Censo Electoral*, 2021, [Tabla]. *Registraduría Nacional, https://www.registraduria.gov.co/-Censo-Electoral-3661-*

El dato total del potencial de personas habilitadas para votar a nivel nacional se obtiene a través de la Registraduría Nacional de Colombia (2021) y es el siguiente:

- Potencial de votos de Hombres: 18,686,306 hombres votantes
- Potencial de votos de Mujeres: 19,935,675 Mujeres votantes
- Potencial Electoral Nacional: 38,621, 981 Total posibles votos a nivel nacional. (Registaduria Nacional del Estado Civil, 2021)

Los datos anteriores son los mismos que se obtienen en la figura 16 y tienen gran importancia porque el diseño de la red está pensado para cubrir la demanda total de los posibles votantes o usuarios que harán uso de este sistema de votación, se conoce que es posible que este número total de personas no voten, pero el diseño de la red se realiza para el caso ideal en que exista una votación de todas las personas a nivel nacional del 100%.

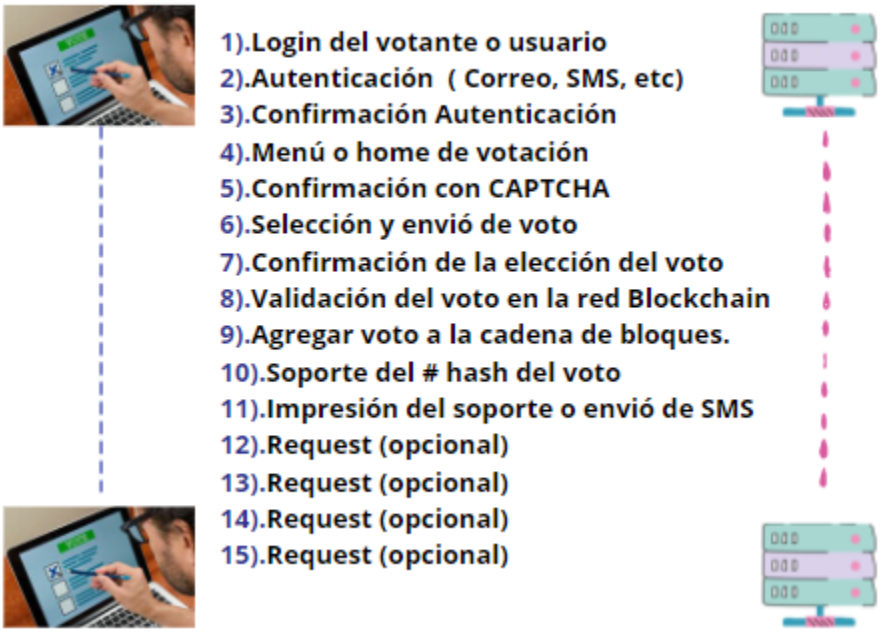
Figura 22. *Potencial Electoral Nacional*

Nota: Adaptada de *Censo Electoral [estadísticas]*, 2021. *Registraduría Nacional, https://www.registraduria.gov.co/-Censo-Electoral-3661-*

5.6.2 *Requerimientos o peticiones al sistema por votante*

Para obtener unos cálculos del coste del sistema muy aproximado se deben tener en cuenta las peticiones que realice cada votante al momento de sufragar, uno de los parámetros es el número de solicitudes (request) que se realicen al nodo o como tal al sistema en general, por eso en la siguiente imagen se detallan las peticiones que cada usuario realizaría al sistema al momento de sufragar.

Figura 23. *Solicitudes*



Nota: Fuente: el autor.

En la imagen anterior, figura 17, se definieron 15 solicitudes (request) para una comunicación que tenga un usuario con el sistema al momento de sufragar. A continuación, se explicará un poco más a detalle cada una de estas:

1. *Login del votante o usuario:* El usuario realiza un *loguin*, como se sabe, el usuario previamente ha sido registrado en el sistema, por ende, el votante debe *loguearse* para entrar al home de la aplicación para poder sufragar.
2. *Autenticación (Correo, SMS, etc):* Por seguridad del usuario y del sistema se debe realizar una autenticación de que la persona que está ingresando realmente es quien dice ser, por tal razón se debe realizar una autenticación de cuenta la cual puede ser con un envió de un código al correo o móvil por mensaje de texto, existen más posibilidades, para este proyecto no se ha definido cual exactamente, pero claramente si se debe realizar una autenticación a la cuenta del usuario que está ingresando a votar.
3. *Confirmación Autenticación:* El usuario debe escribir o realizar el proceso que se defina para la confirmación de su autenticación, por ejemplo, si es por un mensaje de texto que llega al celular seria escribir el código que se le envió.

4. *Menú o home de votación:* Posterior a la autenticación, el usuario ingresa al home de la aplicación en donde encontrara toda la información relacionada a la votación.
5. *Confirmación con CAPTCHA:* Cuando el usuario ingrese al tarjetón para sufragar tendrá que realizar otra validación de seguridad a través de CAPTCHA (Completely Automated Public Turing test to tell computers and Humans Apart) que son pruebas desafío-respuesta controladas por maquinas que son utilizadas para determinar cuando el usuario es un humano o un programa automático.
6. *Selección y envió de voto:* El votante escoge su candidato u opción de los comicios de su ´referencia y selecciona enviar voto.
7. *Confirmación de la elección del voto:* Le aparecerá un mensaje preguntándole que si está seguro de su elección o desea regresar a las opciones. Esto se hace con el fin de una segunda validación de confirmación del voto.
8. *Validación del voto en la red Blockchain:* La red blockchain del sistema recibe y valida que el voto sea efectivo.
9. *Agregar voto a la cadena de bloques:* El voto se agrega a la cadena de bloques del sistema de votación.
10. *Soporte del # hash del voto:* El usuario inicialmente recibirá en la pantalla una confirmación que su voto ha sido agregado a la cadena de bloques efectivamente y obtendrá un número que se llama hash, recordemos que por cada transacción realizada en una red blockchain se obtiene un numero serial que se llama hash el cual es único y hace referencia a la transacción que se agrega a la cadena de bloques.
11. *Impresión del soporte o envió de SMS:* El soporte del voto que es el número del hash el cual le sirve al usuario para que pueda realizar la trazabilidad y verificación que su voto efectivamente está en la cadena de bloques puede ser impreso en un estilo de recibo o como comprobación o certificado de votación o también puede ser enviado como mensaje de texto a su celular o por correo electrónico.
12. , 13, 14, 15). *Request (optional):* Pueden existir casos en los que el usuario por equivocación necesite de más solicitudes, puede existir un error al digitar el código de confirmación o cuando se le pregunta que, si está seguro de su elección, etc. Por este motivo se dejan unas solicitudes adicionales para que el sistema sea redundante.

5.6.3 *Calculo del coste de la solución*

Para el cálculo del coste de la solución se realizará en base a un ejemplo que expone AWS para el cálculo del coste de una red para un servicio en específico, se utilizara este ejemplo que se muestra a continuación como base del cálculo para nuestra red o sistema claramente teniendo en cuenta la información expuesta anteriormente.

5.6.3.1 *Ejemplo de cálculo para un servicio expuesto por AWS:*

1. **Ejemplo de precios**

Para este punto se tendrá en cuenta los datos base que plantea Amazon (2021) en su artículo web “Amazon Managed Blockchain for Ethereum pricing”, justificado mediante un caso planteado por el autor.

Entonces, según el autor: usted es una empresa de eventos que está interesada en unirse a la red principal de Ethereum para registrar y rastrear boletos de eventos. Su aplicación requiere que aprovisione dos nodos c5.large para alta disponibilidad. Cada nodo tiene un libro mayor de 300 GB y se realizan 30 millones de solicitudes a estos nodos durante el mes.

Ahora, teniendo en cuenta los datos base de Blockchain, (Amazon, 2021), se realizan los siguientes procedimientos:

El costo mensual para esto es:

Costo mensual del nodo de pares bajo demanda: 2 X ($ 0.136 por hora X 24 horas) X 30 días = $ 195.84

Costo mensual de almacenamiento del nodo del mismo nivel: 2 X 300GB * X $ 0.10 por GB al mes = $ 60

* Suponiendo que el libro mayor de la red principal es de 300GB

Solicitudes mensuales: 30 millones X $ 3 por millón = $ 90

Costo total mensual: $ 346

Teniendo en cuenta y adaptando el anterior ejemplo que muestra Amazon (2021) para este método de votación que se plantea, se utilizará el mismo nodo de alta disponibilidad llamado C5. Large, como se menciona en el ejemplo anterior. Cada uno de estos nodos tiene un libro mayor de 300GB y soporta 30 millones de solicitudes.

El cálculo que se va a realizar se hará sobre el caso ideal de que el total de personas habilitadas para votar lo hagan, es decir que este costo es sobre la utilización de recursos al 100%. Recordemos que este como varios servicios de AWS se manejan por consumo de recursos y disponibilidad. Lo cual indica que no necesariamente es un valor fijo, pero si es un valor aproximado al coste de la solución planteada.

Lo primero que se realizara es obtener el número total de nodos C5.Large que se necesitan para cubrir la operación a nivel nacional.

- Total posibles votantes a nivel nacional = 38,621,981
- Total solicitudes por votante = 15
- Total de solicitudes en la operación = (38, 621,981 X 15) = 579, 329,715 request.

Obteniendo el número total de solicitudes en el caso más alto e ideal de la operación y conociendo que el nodo C5.Large soporta 30 Millones de solicitudes, se calculara el número de estos nodos que se requiere para cubrir la operación.

- Total de solicitudes en la operación = 579, 329,715 request.
- Un nodo C5.Large atiende = 30,000,000 de request
- Total nodos para cubrir la operación = (579, 329,715 / 30, 000,000) = 19,31 para un aproximado de 20 NODOS C5.Large.

A continuación, se mostrarán los resultados tabulados en la siguiente tabla:

Tabla 3. *Tabulación de Resultados 1*

SERVICIO	**COMPONENTE**	**DETALLE**	**VOTANTES**	**Request por votante**	**Total request**
Peticiones	Peticiones al servidor	Peticiones del usuario a la aplicación para votar.	38,621,981	15	579,329,715

Nota. Fuente: el autor.

Volviendo al calculo que realiza (Amazon, 2021) en su ejemplo, donde utiliza el mismo nodo con la misma capacidad, es de mucha utilidad ya que en ese ejemplo se realiza el cálculo del coste total que tendría uno de estos nodos para atender las solicitudes por un mes, en este punto es válido aclarar que las votaciones actualmente se realizan en un solo día y se plantea que se siga manteniendo así, también recordemos que a Amazon se le cancela por los recursos que se consuman, es decir, se utilizara un día pero se pagara sobre corte de un mes, y de hecho es una opción válida para tener el sistema en funcionamiento por mas días. Después de la aclaración anterior, y retomando el ejemplo de AWS, ya se conoce el coste que tiene uno de los nodos C5.large y a su vez ya se conoce el total de estos nodos que se necesitan para cubrir la operación, es decir que a continuación se realiza el cálculo final del coste aproximado que tendría la red blockchain de la solución.

- Costo total mensual: $ 346 usd por cada nodo C5.Large
- Total nodos C5.Large para la operación: 20

- Total coste operación = ($346 usd X 20 nodos) = $6,920 usd

A continuación, se mostrarán los resultados tabulados en la siguiente tabla:

Tabla 4. *Tabulación de Resultados 2*

COMPONENTE	**DETALLE**	**CANTIDAD TOTAL DE REQUEST**	**CANTIDAD DE REQUEST POR NODO**	**TOTAL NODOS**
Nodo C5.LARGE	Calculo del total de nodos	579,329,715	30,000,000	20

Nota. Fuente: el autor.

En conclusión, para tener una cobertura total de la operación y para un mes de uso de este servicio teniendo en cuenta que se utiliza una vez cada cuatro años a este nivel de votación y a nivel nacional, se obtiene un costo total de $7000 USD aproximadamente para la red blockchain de este método de votación.

A continuación, se mostrarán los resultados tabulados en la siguiente tabla:

Tabla 5. *Tabulación de Resultados 3*

SERVICIO	**COMPONENTE**	**DETALLE**	**COSTE UNITARIO**	**CANTIDAD**	**COSTE TOTAL**
Nodos	C5.Large	Tiene un libro mayor de 300GB y soporta 30 millones de solicitudes.	$346 usd	20	$6,920 usd

Nota. Fuente: el autor.

2. Coste de la solución WEB

Para esta solución y el diseño planteado para esta red también se contempla tener en funcionamiento unos servidores Web que serán en donde se aloje la aplicación con la que el usuario vota, a continuación, se realiza el cálculo del coste de estos servidores.

AWS maneja una instancia que se llama EC2 la cual es una de las más usadas para alojar servicios web de alto rendimiento, ideal para uso en este proyecto y por esta razón se tienen en cuenta para usarse para este proyecto, “Amazon EC2 ofrece la posibilidad de colocar instancias de un mismo proyecto, en distintas ubicaciones que

componen el servicio de Amazon EC2” (Amazon, 2021) . Esto se realiza con el fin de prevenir errores que se produzcan en una zona de disponibilidad específica.

Esta instancia en cuanto a costes se obtiene por hora, y para este ejercicio electoral estos servidores en especial solo tendrán funcionamiento o consumo en las horas de votación de resto permanecerán apagados, para esta solución se tienen pensado un servidor por departamento y en los departamentos con alta demandas como Bogotá, Medellín, Cali y Barranquilla se tendrán de a tres servidores y un conjunto de otros tres servidores para atender las sesiones de los votantes del exterior.

Ejemplo de los costos de las instancias EC2 en AWS:

A continuación, un ejemplo propuesto por Amazon (2021) en su artículo web “Características de Amazon EC2”:

> *“*Por ejemplo, imagine que en algún momento lanza 20 instancias, con un costo de 0,085 USD por hora. Las instancias comenzarán a arrancar inmediatamente, aunque no necesariamente al mismo tiempo. Cada instancia almacenará su hora de lanzamiento real y se empleará este valor para cobrarle (a 0,085 USD/hora) las horas de ejecución reales de cada una de las instancias. Cada instancia se ejecutará hasta que surja uno de estos casos: se termina la instancia con la llamada a la API TerminateInstances (o una herramienta equivalente), la instancia se cierra por sí sola (p. ej., comando “shutdown” de UNIX) o se termina el host debido a un error de software o hardware. Las horas parciales de instancia consumidas se facturan como horas completas en el caso de las instancias de Windows y, en el caso de las instancias de Linux, se facturan por segundo*”* (Amazon, 2021).

Ahora bien, para el caso de este proyecto se usará por cada 500mil usuarios una instancia EC2, en la siguiente tabla se obtiene la cantidad de instancias que se utilizarían por cada lugar, ciudad o departamento.

Tabla 6. *Referencia Censo Registraduría y Total Instancias EC2*

DEPARTAMENTO	**HOMBRES**	**MUJERES**	**TOTAL**	**Numero de servidores WEB (EC2)**
AMAZONAS	26.548	25.034	51.582	1
ANTIOQUIA	2.409.116	2.609.894	5.019.010	10
ARAUCA	108.560	103.219	211.779	1
ATLANTICO	959.593	1.042.103	2.001.696	4

BOGOTA D.C.	2.824.103	3.202.670	6.026.773	12
BOLIVAR	834.830	850.158	1.684.988	3
BOYACA	489.665	501.648	991.313	2
CALDAS	395.265	414.475	809.740	2
CAQUETA	156.462	151.509	307.971	1
CASANARE	152.488	149.113	301.601	1
CAUCA	496.468	516.189	1.012.657	2
CESAR	429.329	436.039	865.368	2
CHOCO	162.183	167.066	329.249	1
CONSULADOS	396.964	463.541	860.505	2
CORDOBA	654.534	659.991	1.314.525	3
CUNDINAMARCA	990.618	1.030.414	2.021.032	4
GUAINIA	16.416	14.772	31.188	1
GUAVIARE	34.916	27.552	62.468	1
HUILA	434.703	442.839	877.542	2
LA GUAJIRA	312.119	330.727	642.846	2
MAGDALENA	507.063	509.738	1.016.801	2
META	385.977	385.102	771.079	2
NARIŃO	571.341	602.140	1.173.481	3
NORTE DE SANTANDER	630.596	664.036	1.294.632	3
PUTUMAYO	121.022	117.531	238.553	1
QUINDIO	234.118	252.359	486.477	1
RISARALDA	395.231	431.241	826.472	2
SAN ANDRES	24.577	26.537	51.114	1
SANTANDER	864.352	904.970	1.769.322	3
SUCRE	366.353	360.906	727.259	2
TOLIMA	549.461	559.386	1.108.847	3
VALLE	1.710.271	1.948.081	3.658.352	7
VAUPES	12.638	10.589	23.227	1

VICHADA	28.426	24.106	52.532	1
			Total servidores Web (EC2)	**89**

Nota. Adaptada de *Censo Electoral*, 2021, [Tabla]. *Registraduría Nacional, https://www.registraduria.gov.co/-Censo-Electoral-3661-*

Como se observa en la tabla anterior, tabla 3, se utilizarían un total de 89 instancias EC2, que según el ejemplo de costo de Amazon tendría un aproximado de *0,85 USD/hora.* Teniendo esto en cuenta el costo sería el siguiente:

1. El horario de votación normalmente es de 8am a 4pm es decir un total de 8 horas.
2. $0,85usd/hora X 8 horas = $6,8usd
3. $6,8usd X 89 instancias = $605,2usd

Como los servidores únicamente se utilizarían un día, basados en las normas de horario del sistema actual, se tiene un costo aproximado de las 89 instancias que cubrirían a nivel nacional un total de $605,2us.

A continuación, se relacionan los datos en la siguiente tabla:

Tabla 7. *Tabulación de Resultados 4*

COMPONENTE	**DETALLE**	**COSTO UNA HORA**	**COSTO 8 HORAS**	**TOTAL INSTANCIAS**	**COSTO TOTAL**
Instancias EC2	Se calcula el aproximado del uso y consumo.	$0,85USD	$6,89USD	89	$605,2 USD

Nota. Fuente: el autor.

Total costos de infraestructura:

A continuación, se dará el costo total aproximado que tendría esta solución o método de votación planteado en este proyecto a nivel de infraestructura de TI, y para el funcionamiento de la red blockchain.

Se sumarán los dos costos que se tienen:

1. Costo total red blockchain
2. Costo total servidores web o instancias EC2.

Lo cual corresponde a:

- $7000USD (Red blockchain) + $605USD (Instancias WEB) = $7.605USD

Es decir que, el valor aproximado que tendría la solución a nivel técnico apoyado en servicios de la nube en AWS sería de $7.605 USD.

Tabla 8. *Tabulación de Resultados 5*

Componente	**Detalle**	**Costo**	**Costo total**
Servicio WEB EC2	Servicio en el que se alojara y funcionara la aplicación web.	$605usd	$605usd
Servicio Blockchain	Servicio en el que se alojara y funcionara la red Blockchain	$7000usd	$7000usd
Servicio Operación día de votación	Se suman los costos de los servicios obtenidos para obtener el valor aproximado total para el día de votación.	N/A	$7605USD

Nota. Fuente: el autor

Costo aproximado del Total de la Operación:

El costo referencia de las votaciones se tiene a partir del costo total del día de las votaciones, es el día y valor que se puede tomar de referencia porque será en el que el consumo y utilización de servicios llegue a su pico más alto. Para esta operación se tienen dos etapas igual de importantes, como lo es el registro de los usuarios o votantes y la auditoria de las elecciones. La única variable que se tiene teniendo en cuenta que es un sistema el cual el costo despende del consumo que se tenga es el tiempo. Para el registro de votantes se propone una semana de utilización, y para la auditoria 3 días, para lo cual el cálculo aproximado de la operación en todas sus etapas tiene un costo aproximado el cual se relaciona en la siguiente tabla:

Tabla 9. *Tabulación de Resultados 6*

COMPONENTE	**DETALLE**	**TIEMPO EN DIAS**	**COSTO DIA**	**COSTO TOTAL**
Etapa de REGISTRO	Etapa de registro de los usuarios o	7	$7,605 usd	$53,235 usd

	votantes			
Etapa de VOTACION	Etapa del día de votaciones.	1	$7,605 usd	$7,605 usd
Etapa de Auditoria	Etapa de auditoria del sistema.	3	$7,605 usd	$22,815 usd
Sistema completo de votación.	Sistema completo de votación con el cumplimiento de las tres etapas.	N/A	N/A	$84,655 USD

Nota. Fuente: el autor.

El costo total aproximado de la infraestructura del sistema de votación planteado en este trabajo de grado con la unión de sus tres etapas tendría un costo de $84,655 USD.

6. Recomendaciones y Aportes de los Beneficios y Aplicativos de la Implementación de Blockchain Especialmente en la Implementación de una Red Blockchain Aplicado a un Ejercicio Electoral a Nivel Colombia.

Para Colombia la tecnología Blockchain no es desconocida, a nivel tecnológico se han tenido interacciones con esta tecnología, como el que se desarrolló en varios colegios de la ciudad de Bogotá en donde ViveLab de la universidad Nacional de Colombia en unión con la Alcaldía de Bogotá desarrollaron elecciones para personeros basadas en la tecnología Blockchain, se destaca la iniciativa en estos ámbitos como al igual el éxito de estas elecciones de personeros en los colegios.

MinTic del gobierno nacional (2021), también mantiene actualmente contacto con la tecnología, por ejemplo entre sus últimos proyectos basados en Blockchain está el apoyo para “la creación de 220 que tengan que ver con Blockchain y analítica de datos, dispuso de 1.399 millones de pesos de financiamiento” (MinTic, 2021), mostrando un acercamiento del gobierno con la tecnología, lo que hace entender que no es desconocida para el gobierno, demostrando un interés y sin descartar esta tecnología por el potencial, futuro, desarrollo y muchos más factores como mejoras para sistemas, un ejemplo es este proyecto ya que tendría un impacto importante en la sociedad.

6.1 Socialización de Usar Tecnología para el Sistema Electoral Actual.

Que la tecnología Blockchain tenga una pedagogía cada vez mayor y más personas, empresas e incluso el mismo gobierno continúen descubriendo el potencial de esta tecnología y todo lo que puede aportar será mucho mejor, como se evidencia en el estudio de la guía de referencia de Blockchain dispuesta por el MinTic (2020).

En Colombia se tiene aún un poco de miedo a lo nuevo, pero este miedo se infunde netamente por falta de conocimiento, es necesario hacer que más personas conozcan la tecnología, beneficios, campos de utilidad, proyección, etc. Entre el conocimiento sea mayor en la sociedad menos miedo se tendrá, y si un sistema electoral basado en Blockchain se presenta como nuevo método para elegir al mandatario o para el caso de Colombia elegir un presidente, teniendo en cuenta que se realizó “la pedagogía adecuada y que las personas realmente conocen el potencial de la tecnología” (Espinosa, 2020), se obtendrá un resultado optimista porque las personas ya confían y conocen lo que el Blockchain aportaría.

Es cierto que en este punto la tecnología sigue estando en desarrollo y que genera incertidumbre, pero a nivel mundial grandes empresas y compañías como Amazon, BBVA, IBM, y más, tienen equipos de ingeniería volcados al desarrollo de servicios basados en esta tecnología, también se conoce de países que son potencia a nivel mundial que están planeando o están estudiando la posibilidad de realizar votaciones electorales basadas netamente en la tecnología Blockchain.

Las iniciativas y proyectos que viene teniendo el gobierno con la tecnología Blockchain tiene un aporte enorme en la socialización que y acercamiento de la tecnología a más personas, no únicamente se enfoca en un área en especial, sino por el contrario, “se está utilizando y desarrollo para títulos de tierra, servicios financieros, votaciones, trazabilidad de alimentos, etc” (Espinosa, 2020). Lo que demuestra el interés del gobierno hacia esta tecnología con gran potencial.

6.2 Diseño y Configuración de la Red Blockchain

El diseño y configuración de la red blockchain es muy importante, y más que una acción en específico se trata de que toda red blockchain requiere de unas reglas y unos estándares especiales basados en el funcionamiento que vaya a tener. Los participantes y directamente responsables del ecosistema electoral deben definir y establecer las configuraciones de la red y el rol de los usuarios como de cada participante de la red, todas las reglas deben estar bien definidas y transparentes para cualquier persona o auditor.

Para un diseño exitoso, como lo indica el artículo web de IT Digital Media Group (2019), se recomienda comenzar con la claridad de la estrategia de negocio, que para este caso no se trata de un negocio como tal que genere rentabilidad, sino que trata de una mejora notable en el método de votación actual y el que se espera a futuro pueda ser implementado y plantado en la sociedad, el valor agregado que aporta un método de votación como este a toda la sociedad de un país entero es bastante por las características en si con que la tecnología blockchain trabaja y que la hacen especial.

Dentro de las configuraciones de la red es muy importante establecer los parámetros y criterios de cada uno de los roles que tomaran todos los participantes de la red, desde el auditor y trabajador, hasta el rol del usuario, esto porque la red será hibrida es decir no del todo será una red pública y tiene algunos permisos auditables por supuesto. Estos permisos y criterios que se configuraran son los que permiten determinar el rol que cumplirá cada participante en la red (IT Digital Media Group, 2019).

Aparte de la configuración que tenga la red acerca de los roles de los participantes la red en su funcionamiento como tal, también cuenta con configuraciones que la caracterizan en su funcionamiento, la hora inicial, la hora final, las reglas de los usuarios habilitados para votar, identificación y criterios para identificar un voto válido y voto nulo, y en sí se recomienda que sea una configuración la cual garantice en toda su totalidad los parámetros, derechos y estándares legales de unas votaciones dentro de las normas a nivel mundial y claramente las normas definidas a nivel nacional.

6.3 Implementación y Redundancia del Sistema

Mediante un estudio detallado de una tesina de grado para magíster en Gestión empresarial de Luis Rodrigo Álvarez (2018), se pudo determinar el siguiente análisis:

Este novedoso sistema de votación se basa en una infraestructura de TI, la cual está pensada y se debe pensar para un uso masivo de personas y con poca tolerancia al fallo, para esta etapa se deben tener en cuenta todos los aspectos técnicos que harán que se haga una realidad este proyecto. El primer factor importante es el protocolo con el que funcionara la red blockchain, por lo reciente de la tecnología no hay un estándar de funcionamiento para la tecnología blockchain, pero si se tienen prototipos muy exitosos y comprobados como el usado para este proyecto, el protocolo tiene una gran escalabilidad lo cual lo hace perfecto para ser tenido en cuenta para una implementación de una red blockchain de este tipo.

Lo segundo a tener en cuenta, es la red blockchain que se usara o sobre la cual se llevaran todos los registros, actualmente existen muchas redes, pero Ethereum es la líder actualmente y con gran proyección a futuro, se encuentra en constante desarrollo y desea lograr grandes cosas con el potencial de la tecnología. Es una de las redes líderes a nivel mundial y por eso trabaja de la mano con AWS para sus servicios basados en la tecnología, se recomienda escoger tanto esta red blockchain como escoger a AWS como proveedor de servicio.

En un sistema de alta escalabilidad e importancia del servicio que presta la infraestructura de TI tiene una importancia mayor, “debe estar a la altura para disponer de una alta disponibilidad del servicio, poca tolerancia a fallos, seguridad, y alta redundancia” (Rojas, 2018); en todo sistema pueden existir fallas técnicas que no deben ocasionar perdida del servicio, para este proyecto una pérdida de servicio por fallas en la infraestructura TI es grave porque tendría impacto directo en la operación al afectar muchas personas que no pueden ejercer su derecho al voto, es por esta razón que se piensa en un mecanismo de redundancia y en el desarrollo de planes de emergencia para implementarlos en caso de que sea necesario.

En cuanto su infraestructura, según lo investigado por Rojas (2018) se afirma que:

“las actividades claves están relacionados a infraestructura TI, seguridad, operación y mantenimiento de aplicaciones y actividades relacionadas a las industrias donde operan. Sus recursos claves son los proveedores de su industria en particular, TI, software, hardware, especialistas en desarrollo y arquitectura, proveedores de plataforma blockchain y comunidades claves” (p. 74).

Así pues, la utilización de los recursos mencionados traza la estructura de costos de estos proveedores del ecosistema.

6.4 Costos Operacionales y Adicionales del Sistema

El sistema de votación que se presenta en este proyecto cuenta con análisis financiero para conocer un aproximado de los costos que tendría desplegar un método de votación de basado en tecnología blockchain, y se aclara que el análisis financiero que se

presenta es netamente a nivel de infraestructura de TI, pero en un despliegue de esta magnitud se debe contemplar varios costes adicionales los cuales se señalaras a continuación:

- *Desarrollo de software y aplicativo de votación:* Este es un costo a tener en cuenta porque el desarrollo del software del sistema y del aplicativo web con el que el usuario va a ejercer su derecho al voto son importantes para el correcto funcionamiento del sistema.
- *Mantenimiento y configuración de la red:* La configuración y mantenimiento de la red se debe llevar a cabo por personal técnico y capacitado para el correcto funcionamiento del sistema, este valor se debe tener en cuenta.
- *Logística del evento:* A pesar de que es un sistema netamente tecnológico, también de manda de personas que estén en la coordinación, inducción, preparación, etc, que demandan un coste adicional para el desarrollo del sistema,
- *Costos operacionales de toda la red:* Los costos operaciones son el conjunto de los costos que se estén omitiendo y que se puedan generar, costos de operación como envió de equipos, seguridad privada o pública como la policía, personal administrativo y demás gastos que demande la operación.

7. Conclusiones

Las características propias de la tecnología blockchain hacen que muchas miradas e interés recaigan sobre ella, es una tecnología que llega a irrumpir con lo tradicional, su forma de red distribuida y no centralizada trae consigo muchos beneficios que la caracterizan como: la trazabilidad de las transacciones que se ejecuten en la red, la seguridad de la información a razón que esta se almacena en bloques y al basarse en criptografía cualquier cambio en la información se verá automáticamente reflejada en toda la red, recordemos que cada transacción se almacena en bloques con un único hash que se compone o se crea de acuerdo a las transacciones que este guarde, es decir cualquier modificación en una transacción cambia automáticamente el hash del bloque dejando de encajar en la cadena, esta acción se ve automáticamente reflejada en toda la red, exponiendo un posible caso de corrupción y ocasionando que los demás nodos de la red la rechacen, esto nos muestra la transparencia de la red porque la información consignada no puede ser modificada, y quizás una de las características más importantes para el uso de un sistema de votación es el anonimato de las personas, lo anterior es posible por las claves públicas del sistema de votación y la clave privada del emisor, es decir la transacción se registra en la red pero no se conoce quien fue la persona dueña de esa transacción, para el caso de este sistema de votación no se conoce quien es la persona dueña del voto, se conoce el voto mas no el sufragante, haciendo que esta y todas las características propias de la tecnología sean ideales para un sistema de votación.

Los sistemas de votación actuales que se utilizan en el mundo tales como el voto tradicional y el voto electrónico, tienen vacíos en su funcionamiento, en especial el voto tradicional que es el más antiguo y que se basa netamente en la confianza del votante en el sistema. La tecnología blockchain en unión a los sistemas que ya se utilizan actualmente puede ser la ficha que hacía falta para tener un sistema electoral perfecto y el cual garantice la trazabilidad del voto y demás características y beneficios que ya se han expuesto en este trabajo. Es por esto que muchos países potencias mundiales se encuentran realizando desarrollos y proyectos de investigación con el fin de sacar el mayor provecho de la tecnología blockchain.

La solución planteada en esta tesis se realiza con la visión de un sistema completo de votación, es decir se debe contemplar todas las variables, factores y actores que interactúen en el sistema, determinando cual es el papel que estos desempeñan dentro del proceso. Para un sistema exitoso también se debe contemplar el proceso anterior al momento de las votaciones y así mismo el proceso posterior, es decir; la solución completa del sistema de votación basado en blockchain. También es importante determinar cada una de las fases que tiene el sistema de votación como el registro de los votantes y auditoria del sistema y de las votaciones, conociendo en qué momento se deben aplicar y las razones por las cuales se debe realizar. Conociendo toda esta

información se piensa en la solución técnica para que se adapte a lo planteado en la gestión de las votaciones.

Actualmente no existe un protocolo estándar bajo el cual el funcionamiento de la tecnología blockchain funcione, para el caso de elecciones a un alto nivel no existe un protocolo sobre el cual permita y exponga el funcionamiento de una red de este tamaño, a nivel mundial se han realizado laboratorios, pruebas y proyectos de este tipo pero con escalabilidad menor, el protocolo que utiliza Ágora, el cual es privado, es funcional demostrado con sus casos de uso hasta el momento y adaptable al nivel de escalabilidad que tiene este proyecto de grado. Esta es la razón principal por la cual se escogió y se explicó este protocolo que ellos utilizan, también se acomoda perfectamente con la gestión de las votaciones, engranando en su totalidad con el fin de proponer un sistema electoral basado en blockchain de alto nivel. Lo ideal es tomar la estructura o funcionamiento de este protocolo como guía y adaptarlo netamente a las necesidades para el funcionamiento pleno del sistema electoral para las elecciones acá en Colombia.

El sistema electoral en toda su totalidad está pensado para que sea implementado en una estructura de la nube utilizando y aprovechando los servicios de blockchain y web de AWS, por coste, seguridad, flexibilidad, etc. La razón principal es que las elecciones presidenciales o cualquier otro tipo de elecciones se llevan a cabo cada determinado tiempo y por lo general solo un día, por esta razón no se piensa en una infraestructura de TI fija o con equipos físicos, sino que por el contrario se piensa en una solución como cloud porque aparte de los beneficios que ofrece, se utiliza la capacidad y se consumen los recursos netamente necesarios y así mismo es el costo.

La tecnología blockchain sigue siendo una tecnología y con muchos cuestionamientos, para tener un punto de referencia el blockchain está en el punto de hace unos años atrás cuando se estaba en los inicios del internet, y todos conocemos los avances que se han tenido no solo en la red de internet sino en la humanidad gracias a esto, se proyecta que en unos años la tecnología blockchain va a ser igual de importante o más a como lo ha sido el internet. Con esta investigación propuesta para este proyecto de grado se obtiene información de relevante para el entendimiento de la tecnología y como sería el uso de la misma para un sistema electoral como el que se planteó para esta. Es importante continuar a la vanguardia de esta tecnología, realizando proyectos e investigaciones a nivel educativo, privado y público como en el gobierno para aprovechar los aportes y beneficios que la tecnología blockchain trae para el mundo.

8. Referencias

1. (UIT), U. I. (11 de 2001). *G.1000 : Calidad de servicio de las comunicaciones: Marco y definiciones*. Obtenido de https://www.itu.int/rec/T-REC-G.1000-200111-I/es

2. Ágora. (10 de 2 de 2021). Ágora Bringing our voting systems. *Whitepaper*. Recuperado el 11 de 2021, de https://shallot-octopus.squarespace.com/s/Agora_Whitepaper.pdf

3. Alcaldía Mayor de Bogotá. (2017). *www.tic.bogotá.gov.co*. Obtenido de Informa Final de Resultado Prototipo Blockchain: http://ticbogota.gov.co/sites/default/files/documentos/blockchain_web.pdf

4. Amazon. (2021). *Características de Amazon EC2*. Colombia. Recuperado el 11 de 2021, de https://aws.amazon.com/es/ec2/features/

5. Amazon. (11 de 2021). Amazon Managed Blockchain for Ethereum pricing. Colombia. Recuperado el 11 de 2021, de https://aws.amazon.com/es/managed-blockchain/pricing/ethereum/

6. BBVA. (5 de 12 de 2017). *www.bbva.com*. Recuperado el 24 de 6 de 2018, de De Alan Turing al "ciberpunk": la historia de "blockchain": https://www.bbva.com/es/historia-origen-blockchain-bitcoin

7. Beamonte, P. (15 de 3 de 2018). *www.hipertextual.com*. Recuperado el 26 de 8 de 2019, de Sierra leona blockchain: https://hipertextual.com/2018/03/sierra-leona-blockchain-elecciones

8. Bermúdez, A. M. (2016). *Estudio de la ultilización de protocolos blockchain en sisitemas de votación electrónica.* Barcelona: Universidad Politécnica de Catalunya.

9. Bit2me. (2021). *Bit2me Academy*. Recuperado el 11 de 2021, de https://academy.bit2me.com/que-es-proof-of-work-pow/

10. Bit2me Academy. (2019). *www.academy.bit2me.com*. Recuperado el 19 de 9 de 2019, de Elecciones Blockchain: ¿se podría votar online?: https://academy.bit2me.com/elecciones-blockchain-votar-online

11. Bitcoin. (11 de 2021). *www.bitcoin.org*. Obtenido de https://bitcoin.org/es/descargar

12. Bitcoin México. (2019). *Bitcoin Mexico*. Obtenido de https://www.bitcoin.com.mx/tokens-para-principiantes/#:~:text=Los%20tokens%20son%20representaciones%20de%20valor%20basados%20en%20Blockchain.&text=Token%20en%20espa%C3%B1ol%20significa%20'Ficha,o%20incluso%20un%20bien%20ra%C3%ADz.

13. Blockchain.com. (11 de 2021). *www.blockchain.com*. Recuperado el 5 de 11 de 2021, de https://www.blockchain.com/es/charts/blocks-size

14. Comunicaciones, M. M. (10 de 11 de 2016). *MinTIC realizó mediciones de calidad en los servicios de telefonía móvil en Bogotá*. Recuperado el 25 de 09 de 2017, de http://www.mintic.gov.co/portal/604/w3-article-22005.html

15. COMUNICACIONES, M. M. (2017). *BOLETÍN TRIMESTRAL DE LAS TIC Julio de 2017.* Recuperado el 02 de 11 de 2017, de http://colombiatic.mintic.gov.co/602/articles-55212_archivo_pdf.pdf

16. Comunicaciones, M. M. (06 de 03 de 2017). *MinTIC amplía plazo para consulta pública de asignación de espectro del Dividendo Digital*. Recuperado el 24 de 10 de 2017, de http://www.mintic.gov.co/portal/604/w3-article-51051.html

17. Criptonoticias. (2 de 11 de 2021). *www.criptonoticias.com*. Obtenido de https://www.criptonoticias.com/criptopedia/como-minar-bitcoin-criptomonedas/

18. Defelipe, S. (21 de 6 de 2018). *www.impactotic.com*. Recuperado el 26 de 8 de 2019, de Blockchain en Colombia sí, criptomoneda no ¿Una nueva versión de #FrenoDigital?: https://impactotic.co/blockchain-en-colombia-si-criptomonedas-no

19. Espinosa, S. (12 de 2020). *Guía de Referentes de Blockchain para la adopción e implementación de proyectos en el Estado colombiano*. Colombia: Ministerio de Tecnologías de la Información y Transformación Digital. Recuperado el 11 de 2021, de https://gobiernodigital.mintic.gov.co/692/articles-161810_pdf.pdf

20. Euskadi.eus. (16 de 11 de 2021). *www.euskadi.eus*. Obtenido de Voto electrónico. Voto electrónico en el mundo: https://www.euskadi.eus/informacion/voto-electronico-voto-electronico-en-el-mundo/web01-a2haukon/es/

21. Evoting. (s.f.). *www.evoting.com*. Obtenido de Voto tradicional Vs. votación online: https://evoting.com/2016/06/08/voto-tradicional-versus-votacion-online//

22. gutierrees, o. (2012). *Bogota.* bogotas: somos.

23. IT Digital Media Group. (11 de 2 de 2019). Cuatro consejos para aplicar blockchain en el entorno empresarial con éxito. Madrid, España. Recuperado el 11 de 2021, de https://www.ituser.es/estrategias-digitales/2019/02/cuatro-consejos-para-aplicar-blockchain-en-el-entorno-empresarial-con-exito

24. Limanorum. (10 de 2018). Recuperado el 9 de 9 de 2019, de Impacto del uso de blockchain en materia electoral: https://www.te.gob.mx/transparencia/media/files/b7156d608ecac4d.pdf

25. Ministerio de Tecnologías de la Información y las Comunicaciones. (30 de 07 de 2019). *Ley 1341 de 2009.* Recuperado el 29 de 09 de 2017, de http://www.mintic.gov.co/portal/604/w3-article-3707.html

26. MinTic. (8 de 2020). *www.mintic.gov.co.* Obtenido de DTL/BLOCKCHAIN: https://mintic.gov.co/portal/715/articles-149959_recurso_1.pdf

27. MinTic. (15 de 6 de 2021). Ministerio TIC formará a 220 empresas en Blockchain y analítica de datos. Colombia. Recuperado el 11 de 2021, de https://mintic.gov.co/portal/inicio/Sala-de-prensa/176599:Ministerio-TIC-formara-a-220-empresas-en-Blockchain-y-analitica-de-datos

28. Morales, A. (2 de 3 de 2021). *enzyme advising group*. Obtenido de https://blog.enzymeadvisinggroup.com/cloud-blockchain-cuatro-grandes-opciones-para-empezar

29. Pastor, J. (21 de 6 de 2016). *www.xataca.com*. Recuperado el 23 de 6 de 2019, de Voto electrónico: éstas son las claves de su fracaso frente a la papeleta de toda

la vida: https://www.xataka.com/especiales/voto-electronico-estas-son-las-claves-de-su-fracaso-frente-a-la-papeleta-de-toda-la-vida

30. Piedra, U. L. (23 de 1 de 2018). *izertis.com*. Obtenido de https://www.izertis.com/es/-/blog/blockchain-seguridad-y-nube-es-posible-apostar-por-ambas

31. Porxas, N., & Conejero, M. (15 de 1 de 2018). *www.uria.com.* Recuperado el 9 de 9 de 2019, de Tecnología blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados: https://www.uria.com/documentos/publicaciones/5799/documento/art02.pdf?id=7875

32. Preukschat, A. (4 de 4 de 2017). *www.iecisa.com*. Obtenido de Tipos de blockchain: https://www.iecisa.com/es/blog/Post/Los-tipos-de-Blockchain-publicas-privadas-e-hibridas-y-II/

33. Registaduria Nacional del Estado Civil. (24 de 11 de 2021). *www.registraduria.gov.co*. Recuperado el 11 de 2021, de https://www.registraduria.gov.co/-Censo-Electoral-3661-

34. Registraduría Nacional del Estado Civil. (2021). *www.registraduria.gov.co*. Obtenido de https://www.registraduria.gov.co/-Glosario-electoral,225-.html

35. Rivero, J. (6 de 3 de 2018). *www.criptonoticias.com*. Recuperado el 26 de 8 de 2019, de Transparencia Electoral: 5 plataformas blockchainvotaciones: https://www.criptonoticias.com/gobierno/votaciones/transparencia-electoral-5-plataformas-blockchain-para-votaciones/

36. Rojas, L. R. (27 de 11 de 2018). Análisis de la Tecnología. 94. Santiago de Chile, Chile: UNIVERSIDAD TÉCNICA FEDERIO SANTA MARÍA. Recuperado el 11 de 2021, de https://repositorio.usm.cl/bitstream/handle/11673/47346/3560900251199UTFSM.pdf?sequence=1&isAllowed=y

37. Semana.com. (30 de 8 de 2019). *www.semana.com*. Recuperado el 9 de 9 de 2019, de Así va el negocio de blockchain en Colombia: https://www.dinero.com/tecnologia/articulo/como-va-el-blockchain-en-colombia/

38. Tapscott, D., & Tapscott, A. (2017). *La revolución blockchain.* Deusto. Recuperado el 4 de 6 de 2019

39. Thilakawardana, M. W. (April de 2012). Initial Analysis of TV White Space. UK: BBC.

40. Wikipedia. (14 de 9 de 2021). *www.wikipedia.com*. Obtenido de https://es.wikipedia.org/wiki/Consejo_Nacional_Electoral_(Colombia)