



BlockID diseño de un sistema de votaciones basado en la tecnología blockchain

Trabajo de grado para optar al título de
Magíster en Ingeniería de Sistemas y Computación

Estudiantes:

Diego Stiven Mejía Herrera
Juan Pablo Múnera Sánchez

Director:

José Alfredo Jaramillo Villegas, PhD.

Universidad Tecnológica de Pereira
Facultad de Ingenierías: Eléctrica, Electrónica,
Física y Ciencias de la Computación
Maestría en Ingeniería de Sistemas y Computación
2022

Índice general

1. Introducción	
1.1. Descripción del problema	7
1.2. Formulación del problema	10
1.3. Objetivos	14
1.3.1. Objetivo General.....	14
1.3.2. Objetivos Específicos	14
1.4. Antecedentes y justificación	14
1.5. Viabilidad y alcance	15
1.5.1. Viabilidad.....	15
1.5.2. Alcance	15
1.6. Metodología	16
1.6.1. Hipótesis.....	16
1.6.2. Diseño Metodológico.....	16
1.6.3. Arquitectura del software.....	16
1.6.4. Desarrollo de software y codificación	17
1.6.5. Pruebas de rendimiento	18
1.7. Sostenibilidad del proyecto	19
1.8. Recursos necesarios	20
1.9. Costo del proyecto.....	20
1.10. Fuentes de financiación	21
1.11. Actividades a desarrollar	21
2. Introducción a la tecnología blockchain	23
2.1. ¿Qué es blockchain?	23
2.2. Conceptos básicos de blockchain.	25
2.2.1. Bloque.	25
2.2.2. Firma digital	26
2.2.3. Billeteras	27
2.2.4. Nodos.	27

2.2.5.	Red Peer to Peer P2P27
2.2.6.	Libros mayores distribuidos - Distributed ledgers28
2.2.7.	Hash28
2.2.8.	Mineros29
2.2.9.	Algoritmos de consenso.29
2.3.	Características principales.31
2.3.1.	Inmutabilidad de los datos31
2.3.2.	Trazabilidad.31
2.3.3.	Verificabilidad32
2.3.4.	Consenso32
2.3.5.	Eliminación de intermediarios33
2.4.	Tipos de blockchain33
2.4.1.	Blockchain Pública33
2.4.2.	Blockchain Privada.34
2.4.3.	Blockchain autorizada o híbrida.35
2.5.	¿Como funciona una blockchain?	36
2.6.	Inicios del blockchain	37
2.7.	Etapas de madurez de la tecnología blockchain.....	38
2.7.1.	Blockchain 1.0.....	39
2.7.2.	Blockchain 2.0.....	39
2.7.3.	Blockchain 3.0.....	40
3.	Sistemas de votación	41
3.1.	El voto.41
3.2.	Sistema de votación o sistema electoral	41
3.3.	Principios fundamentales de los sistemas de votaciones democráticas	42
3.4.	Consideraciones generales de un sistema de votación.43
3.4.1.	Registro de votantes43
3.4.2.	Operaciones de voto44
3.4.3.	Identificación de los votantes.45
3.4.4.	Escrutinio.45
3.4.5.	Auditorías.45
3.5.	Breve Historia del sufragio universal.46
4.	Sistemas de Votaciones Electrónicas	49
4.1.	Sistemas de Votaciones Electrónicas49
4.1.1.	Sistema de tarjetas perforadas50
4.1.2.	Registro Electrónico Directo RED50

4.1.3.	Votaciones por Internet	50
4.2.	Ejemplos de voto electrónico en el mundo	51
4.3.	Sistemas de votaciones basados en tecnología blockchain BVS53	
5.	Descripción de la propuesta	61
5.1.	Propiedades del sistema propuesto	61
5.1.1.	Imparcialidad	61
5.1.2.	Privacidad.....	62
5.1.3.	Verificabilidad	62
5.1.4.	Auditoría.....	62
5.1.5.	Resistencia a la coerción	62
5.1.6.	Usabilidad	63
5.2.	Requerimientos no funcionales	63
5.3.	Stack utilizado.....	64
6.	Arquitectura de software	65
6.1.	Vista de desarrollo - Modelo entidad relación	65
6.2.	Vista de procesos	67
6.2.1.	Diagrama de actividad: Creación de elecciones y candidatos67
6.2.2.	Diagrama de actividad: Votación68
6.2.3.	Diagrama de actividad: Ver resultados69
6.3.	Vista lógica.69
6.3.1.	Diagrama de secuencia: Crear elecciones69
6.3.2.	Diagrama de secuencia: Crear candidato.70
6.3.3.	Diagrama de secuencia: Crear elecciones70
6.3.4.	Diagrama de secuencia: Obtener resultados70
6.4.	Vista física.....	.71
6.5.	Escenarios o casos de uso72
6.5.1.	Caso de uso general.72
6.5.2.	Caso de uso: Generación de candidatos.73
6.5.3.	Caso de uso: Votación74
7.	Pruebas de rendimiento software	75
7.1.	Pruebas de rendimiento de la aplicación	75
7.1.1.	Prueba de Carga (load testing).....	75
7.1.2.	Prueba de Estrés (stress)	76
7.1.3.	Prueba de Resistencia (endurance)	77
7.1.4.	Prueba de Escalabilidad (scalability).....	78

8. Implementación y Conclusiones	79
8.1. Caso de uso	79
8.2. Proceso de elecciones Usuario	79
8.2.1. Creación de cuenta	80
8.2.2. Creación Billetera	83
8.2.3. Selección votación en curso y selección candidato	84
8.3. Proceso de elecciones para el administrador de las elecciones.....	85
8.4. Conclusiones.....	88
Referencias	91

Capítulo 1

Introducción

1.1. Descripción del problema

Las elecciones o votaciones son el pilar fundamental de los sistemas democráticos, ya que permiten a los electores expresar sus opiniones en forma de voto. El voto a su vez es una forma de expresión de la voluntad y deseo de los electores, que sirve para tomar decisiones colectivas. Votar ha sido un método usado desde épocas antiguas y ha sido introducido e implementado ampliamente en la política para elegir las posiciones que ocupan las personas dentro de una sociedad desde hace muchos años y pasando por muchos sistemas y modelos que han ido evolucionando con el tiempo. Los sistemas de votación son la base de todas las elecciones en un país democrático, convirtiéndolas en el núcleo fundamental del proceso democrático [11], la democracia a su vez es una forma de gobierno en la que los ciudadanos de un territorio tienen el poder de decidir las leyes bajo las cuales vivirán. Estas decisiones se toman mediante el voto de los ciudadanos de un territorio a través de una democracia directa, o mediante funcionarios electos por los mismos ciudadanos que deciden en nombre de sus electores en una democracia representativa, tipo de democracia por la cual se rige Colombia. Es importante reconocer también que desde el año 1946 hasta la actualidad el número de países independientes aumentó de 67 a más de 190 [18], muchos de esos países han acogido a la democracia como su sistema político. En la actualidad, se pueden encontrar varios sistemas de votaciones convencionales que van desde los sistemas de votación manual de votos en papel, hasta votaciones en línea o electrónicas. Colombia es uno de los países que aún toma las decisiones electorales con un sistema de votaciones tradicional o de tarjetones, incurriendo en altos costos por impresión de papel y despliegue

logístico, además de la corrupción que se maneja en este proceso tan importante para una sociedad como son las elecciones, ya que muchos procesos han sido objeto de críticas por procesos fraudulentos y procesos manipulados por intereses de ciertos grupos del estado [40], generando además desconfianza en el proceso electoral, debido a la posibilidad de un sistema electoral fraudulento, que se traduce en una forma específica de corrupción dentro del proceso electoral. Por otro lado el voto electrónico ha sido probado o usado a diferentes escalas (referendos, elecciones locales o temas de interés local) en países como: Estados Unidos, Bélgica, Bulgaria, Francia, Alemania, Reino Unido, Holanda, Rusia, Suiza, Estonia (país pionero en las votaciones electrónicas y único país europeo donde el *e-voting* o voto electrónico es usado en elecciones parlamentarias); Estonia, país europeo que ha desarrollado y migrado sus elecciones a un sistema de votación mixto, en donde a los ciudadanos se les permite realizar sus votaciones electrónicas si lo desean, desde cualquier parte del mundo gracias a la facilidad que tienen para votar desde cualquier medio electrónico con acceso a internet como celulares, tablets, o computadores [2], [20]. Sin embargo, este sistema de votación no ha sido muy bien acogido en la comunidad europea y la mayoría de países ha desistido de la implementación oficial de este mecanismo en elecciones nacionales y europeas, esto debido a la posibilidad de hackeo de sistemas electrónicos, problemas con la certificación de resultados electorales y la existencia de errores de software. La desconfianza y el consecuente miedo a que este método se convierta en constitucional han contribuido a la demora del avance.

El principal problema que enfrenta todo sistema de votación es la posibilidad de fraude, el cual está inmerso en el sistema electoral [14]. En otras palabras, se pueden tener unas votaciones limpias con cualquier sistema de votación de los ya existentes, pero las probabilidades de fraude son muy altas debido a la manipulación de la información que se puede dar luego del escrutinio de votos o simplemente por intereses particulares que corrompen las elecciones. Los sistemas de votación convencionales no garantizan la transparencia de las votaciones, ya que históricamente se han visto casos donde el sistema es manipulado para favorecer a un sector en específico de la sociedad [28], [40]. Esta falta de transparencia se traduce en la pérdida de confianza por parte de los votantes y, en consecuencia, esta pérdida de confianza se traduce en altas tasas de abstención [4]; la cual, en el caso de Colombia, siempre está por encima del 50 por ciento [21], lo que quiere decir que el 50 por ciento de los ciudadanos habilitados para votar en Colombia, no participa del proceso electoral. Es de anotar que las posibilidades de

1.2. FORMULACIÓN DEL PROBLEMA

9

1.1. DESCRIPCIÓN DEL PROBLEMA

9

manipulación de los resultados de los procesos electorales no son exclusivos de los sistemas de votación anticuados como las votaciones manuales por medio de tarjetones, como el que se implementa en la mayoría de países democráticos. En Estonia, por ejemplo, durante las elecciones locales del año 2013, se levantaron varias alertas por un potencial riesgo de manipulación sobre el código fuente del sistema de votación electrónico *e-voting* de dicho país, debido a *malware* con capacidad de infectar y manipular las elecciones que entre otras cosas permitía cambiar los votos de los ciudadanos afectando directamente los resultados finales de dichas elecciones [11], este sistema de votaciones electrónicas también ha recibido muchas críticas por expertos en el área, ya que muchas partes del código fuente permanecen ocultas al público, además de las repetidas alertas sobre las debilidades que tiene este sistema con respecto a la seguridad. Como en el año 2002 y 2012 en Estados Unidos se levantaron sospechas en las dos votaciones respectivamente debido a hardware contaminado que afectaba directamente los votos consignados en las máquinas electrónicas designadas para que los votantes expresaran su intención de voto, lo cual levantó las alertas sobre la transparencia de estos sistemas electrónicos. En consecuencia, los sistemas de votación electrónica son alternativas que prometen mucho pero precisan de mejoras en cuanto a la seguridad de la base de datos para garantizar unas votaciones más transparentes.

La Constitución Política Colombiana en sus artículos 1 y 2 proclama la democracia participativa como uno de los pilares bajo los cuales se debe organizar el Estado; la participación política a su vez es lo que fortalece una democracia. Sin embargo, en el caso de Colombia, ha quedado claro, en el registro histórico, que la gran victoria se la ha llevado casi siempre la abstención, que ha estado en casi todas las ocasiones por encima del 50 por ciento, esto, en otras palabras, significa que más del 50 por ciento de los ciudadanos habilitados para votar no hacen uso de su derecho al voto. Según la Ley 892 del año 2004 “Por la cual se establecen nuevos mecanismos de votación e inscripción para garantizar el libre ejercicio de este derecho, en desarrollo del artículo 258 de la Constitución Nacional”, que decretó, entre otras cosas, la creación de un mecanismo de votación electrónico y de inscripción para los ciudadanos colombianos; esta ley aunque no ha sido implementada por el gobierno colombiano, podría facilitar el acceso a los procesos de votación, tanto para los colombianos que habitan en el territorio nacional, así como para los ciudadanos que se encuentran viviendo en el exterior, lo que podría desembocar en una mayor asistencia y/o participación en los procesos electorales.

La aplicación de la tecnología *blockchain* en esta área tiene un gran potencial para mitigar los problemas de manipulación de la información, almacenando la misma en una base de datos descentralizada, donde la seguridad es verificada por nodos públicos de una red y que son imposibles de alterar con el poder computacional existente [10]. De esta forma, la información almacenada en la *blockchain* (cadena de bloques) estará protegida por métodos criptográficos que representan un enorme avance sobre las bases de datos tradicionales, generando de esta manera mayor protección contra los fraudes electorales. Por otro lado, la modernización del voto en Colombia, utilizando la tecnología *blockchain*, podría generar una mayor participación ciudadana, ya que al ser procesos más eficientes y de fácil acceso, se podrían utilizar constantemente para hacer votaciones o sondeos de diferente tipo para generar una mayor inclusión del pueblo en las decisiones de interés común, además de su alto nivel de seguridad, lo que le devolvería la confianza en el proceso electoral a los votantes y podría desencadenar una mayor participación de los votantes.

1.2. Formulación del problema

A pesar de los gigantescos avances tecnológicos y la digitalización de numerosas áreas en la actualidad, la mayoría de las elecciones todavía se llevan a cabo utilizando boletas de papel y, por lo general, fuera de línea, especialmente en las democracias en desarrollo de todo el mundo. La votación tradicional basada en papel o tarjetones tiene los siguientes defectos: los tarjetones de papel son propensos a fraude, existe un margen de error en el conteo manual, problemas logísticos en la distribución de de materiales utilizados en las elecciones de los centros encargados a los puntos de votación, procesos fraudulentos en la gestión de la base de datos de votación, altos costos asociados con la realización de elecciones, consumen mucho tiempo y además sus procesos son muy complejos [14]. Realizar las elecciones de manera electrónica disminuiría drásticamente los gastos de funcionamiento del Estado, también aumentaría la eficacia del proceso, al permitir obtener resultados en el momento que se cierran las urnas con una validez del 100 por ciento de los votos y a su vez mejoraría la seguridad del proceso electoral al usar la tecnología *blockchain*, ya que esta tecnología se basa en la seguridad y transparencia del sistema. Estos sistemas de votaciones electrónicas son ampliamente usados en países desarrollados como Estonia, Estados Unidos, Suiza, entre otros [23]. Sin embargo, estos sistemas aún obligan al estado a disponer las máquinas en un sitio determinado para que los ciudadanos se trasladen hasta él y realicen su voto, el cual queda almacenado en una base de datos bajo el control del ente electoral, lo cual genera muchas dudas sobre la integridad y transparencia de los datos y del proceso electoral como tal.

Uno de los grandes problemas a los que se exponen las bases de datos mencionadas anteriormente son los relacionados con la seguridad y la dispo-

1.2. FORMULACIÓN DEL PROBLEMA

11

nibilidad, de tal forma que una falla en el servidor central de base de datos puede ocasionar la caída de todo el sistema de votaciones, por otro lado, la intrusión a un sistema de base de datos supone grandes riesgos, dado que se podrían modificar los registros de dicha base de datos, lo que supone un gran problema en la veracidad de la información. La estructura de datos *blockchain* sobrepasa estos problemas, proporcionando seguridad de alto nivel al almacenamiento de datos y a la disponibilidad de los mismos. Gracias a la invaluable capacidad de almacenar información inmutable, y que en caso tal de presentarse cualquier variación, aunque sea un solo bit, la base de datos completa se destruye, y se reconstruye a la versión verificada a partir de la información validada por los demás nodos de la red. Estas características son alcanzadas en parte gracias a los avances en criptografía y protocolos de verificabilidad que tiene esta tecnología, generando así un nivel de seguridad que no se había visto antes. Es por esto que la tecnología *blockchain* es una herramienta con un potencial gigante a implementar en los nuevos procesos de votación [6].

En Colombia, la adopción de sistemas electrónicos para realizar votaciones es prácticamente nula, contando con ciertas ayudas informáticas, pero solo de cara a las entidades estatales, y en un porcentaje mínimo (a nivel de visualización de resultados, consulta de jurado y puesto de votación) para uso de la ciudadanía en general. No se esperan grandes cambios en los próximos tres años a esta realidad, sin embargo, en la próxima década (2020-2030), las elecciones electrónicas, implementando la tecnología de la cadena de bloques o *blockchain* tienen un gran potencial de convertirse en la norma para las elecciones populares. No obstante, la adopción de sistemas basados en *blockchain* en Colombia es aún muy baja, teniendo como una de sus principales barreras el desconocimiento de este gran avance de la ciencia de la computación. Evidenciando de esta manera la necesidad de iniciar procesos de sensibilización con ciudadanos y sector gobierno para mostrar abiertamente los alcances de esta tecnología.

Pero no todo es negativo, ya que hay una gran oportunidad con respecto a la modernización de los sistemas de votaciones y los mecanismos de estas, gracias a las iniciativas del Estado para la transformación digital, y es que

para éste la transformación digital del Estado soportado en las tecnologías emergentes es muy importante o por lo menos esto parece en el Plan Nacional de Desarrollo (PND) 2018-2022, ya que la transformación digital es uno de los ejes de mayor importancia para generar un impacto positivo. En el artículo 147 de la Ley 1955 del 2019, Transformación Digital Pública, se define que: “las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. En todos los escenarios la transformación digital deberá incorporar los componentes asociados a tecnologías emergentes, definidos como aquellos de la Cuarta Revolución Industrial, entre otros. Los proyectos estratégicos de transformación digital se orientarán por los siguientes principios:

- Uso y aprovechamiento de la infraestructura de datos públicos, con un enfoque de apertura por defecto.
- Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.
- Plena interoperabilidad entre los sistemas de información públicos que garantice el suministro e intercambio de la información de manera ágil y eficiente a través de una plataforma de interoperabilidad. Se habilita de forma plena, permanente y en tiempo real cuando se requiera, el intercambio de información de forma electrónica en los estándares definidos por el Ministerio TIC, entre entidades públicas. Dando cumplimiento a la protección de datos personales y salvaguarda de la información.
- Optimización de la gestión de recursos públicos en proyectos de Tecnologías de la Información, a través del uso de los instrumentos de agregación de demanda y priorización de los servicios de nube.
- Promoción de tecnologías basadas en software libre o código abierto, lo anterior, sin perjuicio de la inversión en tecnologías cerradas. En todos los casos la necesidad tecnológica deberá justificarse teniendo en cuenta análisis de costo-beneficio.
- Priorización de tecnologías emergentes de la Cuarta Revolución Industrial que faciliten la prestación de servicios del Estado a través de

nuevos modelos incluyendo, pero no limitado a, tecnologías de desintermediación, DLT (*Distributed Ledger Technology*), análisis masivo de datos (*Big data*), inteligencia artificial (AI), Internet de las Cosas (IoT), Robótica y similares.

- Vinculación de todas las interacciones digitales entre el Estado y sus usuarios a través del Portal Único del Estado colombiano.
- Implementación de todos los trámites nuevos en forma digital o electrónica sin ninguna excepción, en consecuencia, la interacción del Ciudadano-Estado sólo será presencial cuando sea la única opción.
- Implementación de la política de racionalización de trámites para todos los trámites, eliminación de los que no se requieran, así como en el aprovechamiento de las tecnologías emergentes y exponenciales.
- Inclusión de programas de uso de tecnología para participación ciudadana y Gobierno abierto en los procesos misionales de las entidades públicas.
- Inclusión y actualización permanente de políticas de seguridad y confianza digital.
- Implementación de estrategias público-privadas que propendan por el uso de medios de pago electrónicos, siguiendo los lineamientos que se establezcan en el Programa de Digitalización de la Economía que adopte el Gobierno nacional.
- Promoción del uso de medios de pago electrónico en la economía, conforme a la estrategia que defina el Gobierno nacional para generar una red masiva de aceptación de medios de pago electrónicos por parte de las entidades públicas y privadas.

Aunque no todos los puntos de este Plan Nacional De Desarrollo, se refieren al proyecto de referencia, se puede evidenciar la intención del Estado de utilizar tecnologías nuevas para optimizar y mejorar los procesos públicos, lo cual es una gran oportunidad para las nuevas tecnologías en pro de la sociedad colombiana. La popularidad que obtiene esta tecnología *blockchain* gracias a las criptomonedas puede ser un factor fundamental para la implementación de esta tecnología en nuevos procesos y nuevas áreas de función pública, y es que para los próximos años esta tecnología tiene un valor agregado en cuanto a la seguridad e integridad de la información; todo esto sumado al

descontento y falta de credibilidad en el proceso electoral que existe en Colombia.

1.3. Objetivos

1.3.1. Objetivo General

Construir, desplegar y evaluar un sistema de votaciones electrónicas privadas usando la tecnología *blockchain*.

1.3.2. Objetivos Específicos

- Analizar los requerimientos del sistema de votaciones.
- Construir las vistas 4+1 del sistema de votaciones.
- Desarrollar y desplegar el software del sistema de votaciones diseñado.
- Realizar pruebas de rendimiento al sistema de votaciones desplegado.

1.4. Antecedentes y justificación

La tecnología avanza a gran velocidad, hoy en día todas las áreas de gestión del Estado están sujetas a la sistematización, lo que supone una gran ventaja, pero al mismo tiempo un peligro para la seguridad de los datos. Los sistemas *blockchain* pueden aportar un gran avance al sistema electoral, tanto de instituciones, como de empresas u organizaciones en general en Colombia, simplificando la manera en la que se llevan las elecciones populares, generando grandes ahorros de dinero y redundando en la seguridad de los datos.

De esta manera la tecnología *blockchain* puede aportar una solución eficiente a la forma en la que se realiza una elección popular. Esto gracias a la característica inmutable de los datos consignados en este tipo de estructura de datos [6]. Dicha inmutabilidad permite a los electores estar tranquilos de que su voto no va a ser adulterado ni compartido, además, los usuarios podrán conocer los resultados de las elecciones en tiempo real. Brindando de esta manera mayor transparencia y confianza en el proceso electoral.

Es por lo anterior, que se propone iniciar con la investigación y el desarrollo de un sistema de votaciones basado en *blockchain*, con el fin de probar las ventajas y desventajas de un sistema de este tipo, a través de un

prototipo funcional adaptado para ser usado en cualquier tipo de votación digital. En un principio, lo que se busca es poder difundir estos sistemas de votaciones y alcanzar una notoriedad importante en la comunidad con la intención de que esta tecnología y sus beneficios se den a conocer. El alcance de este proyecto llegará hasta la implementación, despliegue y evaluación de sistemas de votaciones privadas de pequeños y medianos grupos de personas, debido a la limitante de tiempo, recursos y permisos que se requiere para escalar estos sistemas de votaciones a unas elecciones de alcalde o gobernador por ejemplo.

1.5. Viabilidad y alcance

1.5.1. Viabilidad

El sistema a desarrollar se basará en librerías de código abierto (*Multichain*), lo que evitará gastos extras en licenciamiento. Por otro lado, la construcción del software se realizará con base en la metodología XP (*Extreme Programming*), con el objetivo de agilizar el proceso de desarrollo. El proyecto está pronosticado para finalizar en ocho meses y todos los recursos físicos, logístico y humanos han sido calculados para este periodo de tiempo.

1.5.2. Alcance

La presente investigación llegará hasta la implementación de un sistema de votaciones privadas utilizando la tecnología *blockchain*. Específicamente se construirán los siguientes módulos:

- Gestión de identidades digitales.
- Verificación de firmas digitales emitidas por la *blockchain*.
- Construcción de tarjetones electrónicos.
- Votación de las opciones generadas.
- Generación de certificados electorales.
- Visualización de resultados en tiempo real (una vez terminadas las elecciones).

1.6. Metodología

1.6.1. Hipótesis

Es posible crear un sistema de votación basado en la tecnología *block-chain*, con una interfaz fácil de manejar para los usuarios, de manera que estos puedan crear elecciones y obtener estadísticas de las votaciones.

1.6.2. Diseño Metodológico

1.6.3. Arquitectura del software

El primer paso consiste en construir el modelo de vistas de arquitectura 4+1 para describir la arquitectura de sistemas software propuesto, este modelo de vistas consiste en el uso de múltiples vistas concurrentes para describir el software desde distintos puntos de vistas, están enfocados en cada una de las diferentes partes interesadas: usuarios finales del software, programadores, administradores del proyecto, entre otros. Cada punto de vista de una arquitectura representa un subconjunto de componentes que interactúan entre sí, provenientes de una o varias estructuras con una función o significado particular dentro del sistema. En el modelo se proponen cuatro vistas principales: vista lógica, vista de desarrollo, vista física y vista de procesos, y una vista adicional utilizada para unir las otras que es la vista de escenarios o casos de uso que se utiliza para validar el diseño de la arquitectura [25].

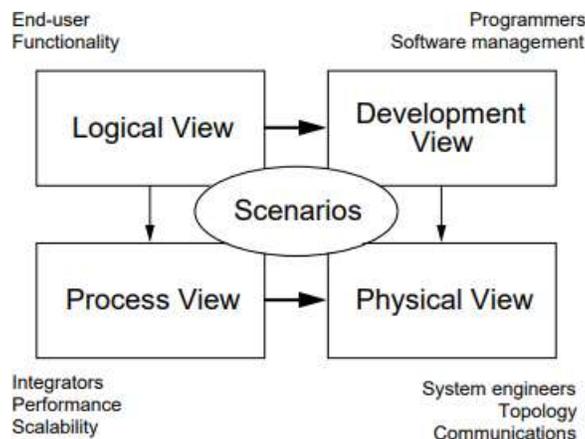


Figura 1.1. Modelo de vistas de arquitectura 4+1 [25].

- Vista lógica: la vista lógica describe el modelo de objeto del diseño cuando se utiliza un método de diseño orientado a objetos. Para diseñar una aplicación que esté muy basada en datos, puede utilizar un enfoque alternativo para desarrollar alguna otra forma de vista lógica, como un diagrama de relación entre entidades [25].
- Vista de procesos: la arquitectura de procesos describe algunos requisitos no funcionales como la disponibilidad y el rendimiento. Se diseña con base a asuntos de concurrencia, distribución, integridad del sistema y tolerancia a las fallas que puedan ocurrir en los procesos. La vista de procesos también especifica en qué punto se ejecuta efectivamente una operación de una clase identificada previamente en la vista lógica.
- Vista de desarrollo: la vista de desarrollo se centra en cómo están organizados los módulos de software en el ambiente de desarrollo del software, esta vista está enfocada para mostrar a los programadores y administradores del software la estructura. El software se empaqueta en partes pequeñas que van desde bibliotecas de programas a subsistemas que pueden ser desarrollados. Los subsistemas se organizan en forma de jerarquía de capas, cada una de las capas brinda una interfaz estrecha y bien definida hacia las capas superiores [25].
- Vista física: la vista física se encarga principalmente de mapear el software al hardware, ya que en esta vista se toman en cuenta los requisitos no funcionales del sistema: tolerancia a fallas, rendimiento, disponibilidad, escalabilidad, etc. Por lo general, los software se ejecutan sobre una red de computadores o nodos de procesamiento. El mapeo del software en los nodos establecidos requiere un impacto mínimo sobre el código fuente y ser altamente flexible [25].
- Escenarios o casos de uso: este tipo de vista es redundante con las otras 4, por eso significa el +1 del modelo y funciona como guía para descubrir elementos de arquitectura durante el diseño, pero también sirve para validar e ilustrar después de completar todo el diseño de la arquitectura del software realizada previamente, también es el punto de partida para las pruebas del prototipo de la arquitectura [25].

1.6.4. Desarrollo de software y codificación

Se inicia con el despliegue de una *blockchain* privada sobre dos servidores con GNU/Linux. Este par de nodos funcionan como mineros de la *blockchain*

y como nodos de almacenamiento de los bloques producidos. Los bloques se generarán a una tasa de un bloque cada 30 segundos, con un tope máximo de 4 MB de información por bloque, y con una condición de parada de un máximo de 30 bloques vacíos para ahorrar energía y espacio en disco. Esto quiere decir que, luego de minar 30 bloques sin ninguna transacción, la *blockchain* entrará en estado de suspensión para evitar seguir generando más bloques vacíos. Esta es una de las condiciones características de las *blockchain* privadas, que por su naturaleza no son utilizadas las 24 horas del día.

Luego de tener la *blockchain* funcionando, se procede al desarrollo e implementación de un software para interactuar con la misma y desde allí construir la lógica necesaria para escribir y leer la información requerida para el desarrollo de las votaciones. Los módulos de software que se van a desarrollar deben permitir gestionar las identidades de los votantes, los candidatos (personas u opciones) y las estadísticas de la votación en curso.

1.6.5. Pruebas de rendimiento

Las pruebas de rendimiento son una técnica de prueba de software no funcional que miden el comportamiento, la estabilidad, la velocidad, la escalabilidad y la capacidad de respuesta de una aplicación cuando es sometida a determinadas cargas de trabajo. Se realizaron las siguientes pruebas de rendimiento al sistema para ver cómo era su comportamiento con altas cargas de trabajo:

- Carga (*load testing*): tiene como objetivo comprobar la cantidad de peticiones concurrentes que el sistema puede soportar. Se utilizará un software para generar una cantidad masiva de peticiones al software y de esta manera comprobar la carga que el mismo puede soportar.
- Estrés (*stress*): consistirá en enviar más peticiones a las esperadas en condiciones normales de operación, para conocer el comportamiento del sistema en este tipo de situaciones. Se utilizará un software para generar una cantidad de peticiones mayor a la soportada para verificar el comportamiento del sistema.
- Resistencia (*endurance*): se comprobará la estabilidad y funcionamiento del software posterior a las pruebas de estrés.
- Escalabilidad (*scalability*): permitirá evaluar e identificar las mejoras a la infraestructura donde reside la aplicación. Para este fin, se van a

monitorear los recursos del sistema, tales como memoria RAM, procesadores y ancho de banda.

1.7. Sostenibilidad del proyecto

La *blockchain* que se va a utilizar en el proyecto fue creada en la plataforma de Multichain y está licenciada con GPLv3 (<https://www.gnu.org/licenses/gpl-3.0.html>), lo cual exige que los productos de software que se desarrollen con esta *blockchain* también se deben liberar bajo la misma licencia de código abierto. Esto constituirá un aporte a la comunidad de software libre, ya que se liberará todo el código del sistema de votaciones basado en la *blockchain* de Multichain para que la comunidad lo pueda copiar, modificar y redistribuir.

Dicho lo anterior, la red *blockchain* a utilizar permitirá configurar una arquitectura privada, es decir, el equipo de desarrollo tendrá pleno control sobre la red y no se permitirá que cualquier usuario se convierta en minero de la red desplegada. Esto conlleva una ventaja económica que impacta directamente en la sostenibilidad, ya que no se incurrirá en costos por transacción, solo los costos por servidores, los cuales serán asumidos por la empresa que está patrocinando el proyecto (Pulsatrix) y por los desarrolladores del proyecto.

Desde el punto de vista social, este proyecto aporta a una discusión pendiente en el país: la modernización del sistema de votaciones actual y la transparencia del mismo. Esta tecnología tiene un potencial disruptivo que podría cambiar la sociedad como la conocemos, aunque los problemas con respecto a la corrupción de los sistemas de votación no son exclusivos del sistema de votación, sino a la estructura de la misma, teniendo o implementando esta tecnología *blockchain* implementada en el sistema de votación se reduciría ese margen de acción para los corruptos y se podría devolver esa confianza al elector en su sistema de votación, lo cual seguramente se vería traducido en tasas de asistencia más altas a las elecciones. Si bien se trata de un sistema en fase inicial, también es una prueba de concepto sobre las posibilidades que tienen los sistemas de votación basados en *blockchain*.

Desde el punto de vista ambiental, este tipo de sistemas puede tener un aporte muy importante dentro de la sociedad y es que al ser desplegados de manera masiva para llevar a cabo elecciones formales, como elecciones de alcaldías, parlamentarias o presidenciales, podría modernizar este proceso desde su estructura hasta sus mecanismos y es que el gasto de recursos que

conlleva una elección son gigantes, ya que incluyen tanto recursos logísticos como recursos físicos como papel y tinta [36].

1.8. Recursos necesarios

- **Recursos físicos:** dos (2) servidores virtuales de 4 GB de RAM, tres (3) núcleos de procesamiento y veinte (20) GB de disco para el funcionamiento de la *blockchain* privada por 8 meses.
- **Recursos lógicos:** implementación de la tecnología *blockchain* con base en la plataforma MultiChain (plataforma *blockchain* de código abierto), herramientas de software: nodejs + Express (Backend), Ionic + angular (Frontend), Obtención de espacios en donde se puedan desarrollar pruebas al prototipo del software.
- **Recursos humanos:** asesoría de un (1) profesor UTP y dos (2) ingenieros dedicados al proyecto.

1.9. Costo del proyecto

Los costos mencionados a continuación son por el tiempo de 8 meses, que se pronostica que durará el proyecto, y en su mayoría serán suministrados por la empresa Pulsatrix, patrocinador oficial de este proyecto.

	TIPO	DESCRIPCIÓN	VALOR Aprox. (COP)
RECURSOS FÍSICOS	Variable	Dos (2) servidores virtuales de 4GB de RAM, tres (3) núcleos de procesamiento y veinte (20) GB de disco.	\$1'000.000
RECURSOS LÓGICOS	Fijo	Acceso a la plataforma Multichain, herramientas de software: Nodejs + Express (Backend) , Ionic + angular (Frontend), pruebas del software.	\$1'000.000
RECURSOS HUMANOS	Variable	Asesorías profesor UTP, costo de los dos ingenieros dedicados al proyecto.	-
TOTAL	-	Costos totales incluyendo un sobrecosto del 20% que cubrirá los imprevistos en caso de tenerlos	\$2'400.000

Figura 1.2. Costo del Proyecto.

1.10. Fuentes de financiación

La principal fuente de financiación es la empresa Pulsatrix, patrocinadora oficial de este proyecto y aliado estratégico que aportará la mayoría de los recursos del proyecto, se espera obtener también la colaboración directa de la Universidad Tecnológica de Pereira para facilitar el personal humano necesario para las asesorías y guía del proyecto. Los cálculos fueron realizados para un intervalo de tiempo de 8 meses que durará el proyecto.

1.11. Actividades a desarrollar

Objetivo 1. Identificar los requerimientos fundamentales y estándares para los sistemas de votaciones, de ahí se hará un análisis si son las mismas condiciones requeridas en las votaciones públicas y privadas, utilizando la tecnología *blockchain*.

- Aproximación al estado del arte.
- Marco teórico.
- Identificación de los requerimientos generales para votaciones de orden privado.

Objetivo 2. Analizar los requerimientos del sistema de votación y marco teórico.

- Análisis del estado del arte, marco teórico y requerimientos generales para votaciones públicas y privadas usando tecnología *blockchain*.
- Planeación y definición de actividades a realizar en software previsto para votaciones públicas y privadas.
- Definición de requerimientos generales para sistemas de votación públicos y privados.

Objetivo 3. Construir las vistas 4+1 para describir la arquitectura del sistema software, basado en el uso de múltiples vistas concurrentes para describir el punto de vista para los diferentes interesados del proyecto.

Objetivo 4. Desarrollar el software y la codificación.

- Desplegar una *blockchain* privada sobre la cual se va a desarrollar el sistema.
- Construir una aplicación web para interactuar con la *blockchain* privada y permitir que el usuario emita un voto a través de una interfaz gráfica sencilla.
- Construir un panel de administración para permitir la creación de las opciones de votación.

Objetivo 5. Realizar pruebas de rendimiento del software.

- Carga (*load testing*).
- Estrés (*stress*).
- Resistencia (*endurance*).
- Escalabilidad (*scalability*).

Capítulo 2

Introducción a la tecnología *blockchain*

2.1. ¿Que es *blockchain*?

Una cadena de bloques consiste en conjuntos de datos que se componen de una cadena de paquetes de datos ó bloques de datos, las cuales almacenan múltiples transacciones validadas previamente por la red. La cadena de bloques se amplía con cada bloque adicional y, por lo tanto, representa un registro completo del historial de transacciones de principio a fin. Los bloques pueden ser validados por la red utilizando medios criptográficos. Además de las transacciones, cada bloque contiene una marca de tiempo, el valor *hash* del bloque anterior y un *nonce*, que es un número aleatorio para verificar y generar el *hash*. Este concepto garantiza la integridad de toda la cadena de bloques desde el primer bloque de la cadena “bloque genesis” hasta el último bloque minado. Los valores hash son únicos e irrepetibles y el fraude se puede detectar y prevenir de manera efectiva, ya que cualquier cambio en la información que contiene un bloque, por más mínimo que sea, cambiaría inmediatamente el valor del *hash* respectivo. Si la mayoría de los nodos de la red acuerdan mediante un mecanismo de consenso (definido para cada una de las *blockchain*) sobre la validez de las transacciones en un bloque y sobre la validez del bloque en sí mismo, el bloque se puede agregar a la cadena. Este proceso de consenso es muy importante dentro de lo que significa la *blockchain* ya que es el proceso en el que la mayoría ó todos de los validadores de la red llegan a un acuerdo sobre el estado del libro mayor. Es un conjunto de reglas y procedimientos que permite mantener un conjunto coherente de hechos entre múltiples nodos participantes.

24CAPÍTULO 2. INTRODUCCIÓN A LA TECNOLOGÍA BLOCKCHAIN

Por lo tanto, las nuevas transacciones no se agregan automáticamente a el libro mayor, más bien, el proceso de consenso garantiza que estas transacciones se almacenen en un bloque durante un tiempo determinado, por ejemplo, 10 minutos en la cadena de bloques de Bitcoin antes de transferirse al libro mayor. Posteriormente, la información en la cadena de bloques ya no se puede cambiar. En la mayoría de *blockchains*, los bloques son creados por los llamados mineros que son recompensados con algún tipo de remuneración, en el caso de *blockchain* los mineros reciben un porcentaje de un Bitcoin por validar los bloques. La cadena de bloques no solo puede cambiar el proceso de las transacciones monetarias, ya que al usar la criptografía y mecanismos de consenso, las personas de todo el mundo pueden confiar entre sí y transferir diferentes tipos de activos entre pares a través de Internet con altos niveles de transparencia y seguridad [34], [35].

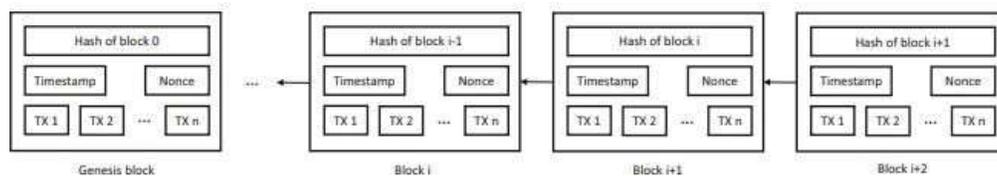


Figura 2.1. Ejemplo de una *blockchain* [43].

La tecnología *blockchain* como agente disruptivo de la sociedad ha tomado mucha fuerza en los últimos años y ha generado el interés de las grandes empresas, gobiernos y la academia para su implementación en múltiples proyectos y áreas de la industria [3], [33], [16]. Es importante también aclarar que las criptomonedas se basan en la tecnología *blockchain* teniendo como su máximo exponente el Bitcoin, pero a su vez esta tecnología no se limita solo a las criptomonedas, en realidad esta ofrece una manera segura para el intercambio de casi cualquier bien, servicio o transacción y, además, tiene muchas aplicaciones, entre las cuales se encuentran: internet de las cosas, servicios financieros, almacenamiento en la nube, registro y verificación de datos, contratos inteligentes, cadenas de suministro, seguridad automatizada, sistemas de votación, entre muchas otras aplicaciones [3], [16].

Esta tecnología *blockchain* tiene la capacidad y potencial para transformar los sistemas y procesos tradicionales en el panorama económico, servicios públicos, legal, político y cultural de la actualidad, en sistemas más seguros, transparentes y colaborativos que a su vez acercan y empoderan a sus usuarios [1]. La revolución tecnológica que se está viviendo en los últimos años, sumada a una sociedad colaborativa y participativa podría llevar a la

creación y/o formación de comunidades distribuidas y de consenso independientes de terceros de confianza organizados jerárquicamente [33]. En realidad, ya se está viendo que las aplicaciones que comúnmente se ejecutaban a través de un intermediario de confianza, ahora pueden operar de manera descentralizada [12], sin necesidad de tener autoridad central siendo su caso más emblemático el uso de criptomonedas.

2.2. Conceptos básicos de *blockchain*

2.2.1. Bloque

Los bloques son simplemente paquetes de datos que contienen información de transacciones que suceden en la red en un tiempo determinado. Los bloques generalmente incluyen estos elementos, pero pueden variar entre los diferentes tipos de *blockchain*:

- *Blocksize* o tamaño de bloque: como su nombre lo indica, establece el límite de tamaño en el bloque para que solo se pueda escribir una cantidad específica de información en él.
- Encabezado del bloque: contiene información sobre el bloque.
- Contador de transacciones: este es un número que representa cuántas transacciones se almacenan en el bloque.
- Transacciones: una lista de todas las transacciones dentro de un bloque.

El encabezado del bloque es sumamente importante e incluye los siguientes subelementos:

- Versión: la versión de la *blockchain* que se está utilizando.
- *Hash* del bloque anterior: contiene un *hash* del encabezado del bloque anterior.
- Raíz Merkle: *hash* de transacciones en el árbol Merkle del bloque actual.
- Hora: una marca de tiempo para colocar el bloque en la cadena de bloques.

26CAPÍTULO 2. INTRODUCCIÓN A LA TECNOLOGÍA BLOCKCHAIN

- Bits: la calificación de dificultad del *hash* de destino, lo que significa la dificultad para resolver el *nonce*.
- *Nonce*: El número encriptado que debe resolver un minero para verificar el bloque y cerrarlo.

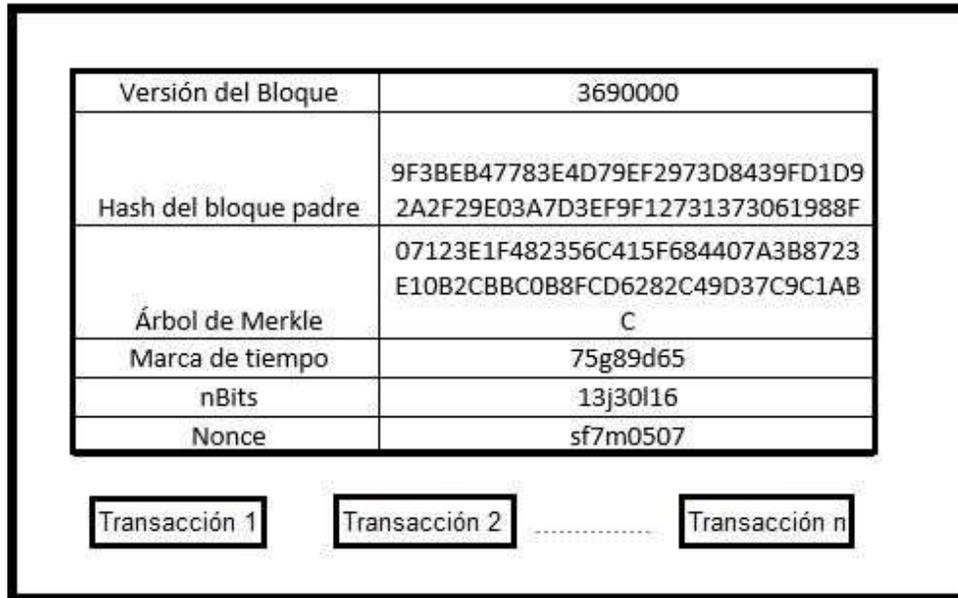


Figura 2.2. Estructura de un bloque [43].

2.2.2. Firma digital

Cada usuario posee un par llaves denominadas clave privada y clave pública. La clave privada se utiliza para firmar las transacciones, las transacciones firmadas digitalmente se distribuyen por toda la red y luego se accede a ellas mediante claves públicas, que son visibles para todos en la red. La firma digital típica se divide en dos fases: la fase de firma y la fase de verificación. Cuando un usuario quiere firmar una transacción, primero genera un valor *hash* derivado de la transacción, luego encripta este valor *hash* usando su clave privada y envía a otro usuario el *hash* encriptado con los datos originales, este verifica la transacción recibida a través de la comparación entre el *hash* descifrado (usando la clave pública del remitente) y el valor

hash derivado de los datos recibidos por la misma función hash que la del remitente.

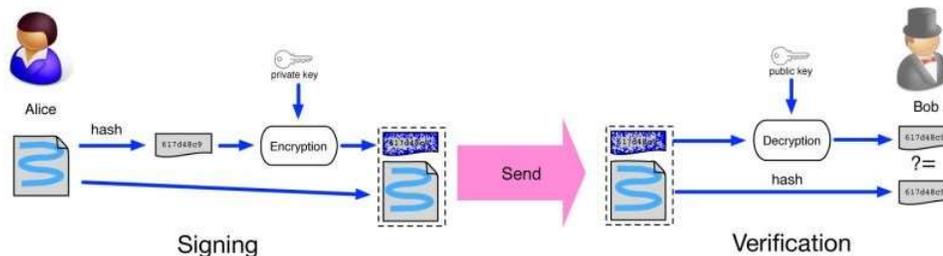


Figura 2.3. Firma digital [43].

2.2.3. Billeteras

Una billetera *blockchain* es una billetera digital que permite a los usuarios almacenar y administrar sus activos, esto quiere decir que la billetera brinda la posibilidad a los usuarios de interactuar con sus activos dentro de la *blockchain* para enviar o recibir activos, pero en realidad estos activos están almacenados en la *blockchain*.

2.2.4. Nodos

Los nodos representan agentes o participantes en una red de cadena de bloques. Dependiendo de los permisos establecidos en la red, pueden aprobar, validar, enviar o recibir transacciones y datos. Los nodos también almacenan una copia completa del libro mayor distribuido y son responsables de la confiabilidad de los datos almacenados. Gracias a los nodos de *blockchain*, cualquier usuario puede acceder a los datos y puede ver todas las transacciones realizadas o almacenadas en la red.

2.2.5. Red Peer to Peer P2P

Una red P2P o par a par, es una arquitectura informática distribuida en la que los distintos nodos que componen esta red comparten entre ellos parte de sus recursos informáticos, como: potencia informática, espacio de disco duro y RAM, ancho de banda, entre otros, sin necesidad de un nodo central que supervise todo, los nodos de esta red no están jerarquizados entre

cliente-servidor, sino que son iguales y a su vez capaces de realizar el rol de cliente y de servidor a la vez. Una de las principales ventajas de este tipo de red es que es más sólida frente a contingencias que pudieran ocurrir, ya que todos los nodos funcionan de forma independiente.

2.2.6. Libros mayores distribuidos - *Distributed ledgers*

Un libro mayor distribuido es una base de datos que se comparte y sincroniza de forma consensuada entre varios sitios, instituciones o zonas geográficas, a la que pueden acceder varias personas. Esos libros mayores distribuidos permiten que las transacciones tengan testigos públicos. El participante en cada nodo de la red puede acceder a las grabaciones compartidas a través de esa red y puede poseer una copia idéntica de la misma. Cualquier cambio o adición realizada al libro mayor se refleja y se copia a todos los participantes de la red en cuestión de segundos o minutos.

2.2.7. Hash

Una función criptográfica *hash* o *hash* es el resultado de aplicar una algoritmo matemático que transforma un bloque arbitrario de datos en una nueva serie de caracteres con longitud fija. Algunas de las características principales de estas funciones *hash* son:

- Irreversibilidad: esta característica es muy importante, y también es la que más distingue al hashing, que es irreversible, ya que conociendo el hash, es matemáticamente imposible deducir el texto original.
- Determinismo: la entrada **A** produce y siempre producirá el mismo *hash* **B**. Las funciones *hash* son deterministas precisamente porque la salida de una entrada fija es siempre la misma.
- Longitud fija: la salida producida por las funciones *hash* tiene una longitud fija siempre a un mismo número de caracteres.
- Efecto avalancha: el efecto de avalancha es una propiedad por la cual un pequeño cambio en la entrada **A** produce un cambio notable en los *hashes*.

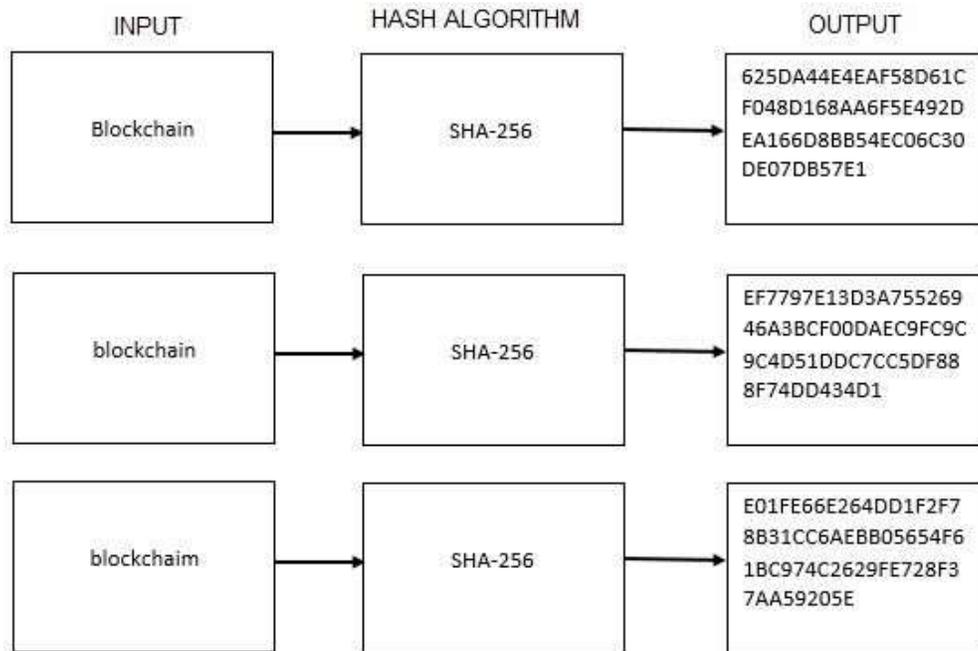


Figura 2.4. Ejemplo de función *hash* utilizando *secure hash algorithm 256* SHA256.

2.2.8. Mineros

Algunos nodos de la red *blockchain* participan en resolver un algoritmo de consenso, aquellos nodos que participan en la búsqueda de la solución de estas pruebas reciben el nombre de mineros, además son los encargados de crear nuevos bloques. Cada vez que un minero consigue minar un bloque, este recibe una recompensa por su esfuerzo en las *blockchain* públicas. Al ser una red descentralizada, es la misma red la que paga o incentiva a estos nodos para que trabajen en la red.

2.2.9. Algoritmos de consenso

Al ser el *blockchain* una base de datos distribuida, la validación de los datos en ella no se realiza desde un nodo central o un tercero de confianza, sino a través del consenso de todos los participantes de la red. Este consenso es alcanzado a través de la implementación de algoritmos de validación que, a su vez, son guía de los mineros de la red para verificar las transacciones y minar los bloques. Entre los algoritmos de consenso más usados en las

30CAPÍTULO 2. INTRODUCCIÓN A LA TECNOLOGÍA BLOCKCHAIN

cadenas de bloques se encuentran: prueba de trabajo (PoW), prueba de participación (PoS), Prueba de participación delegada (DPoS), prueba de tiempo transcurrido (PoET), entre otros [31].

- Prueba de trabajo (PoW): este algoritmo de consenso es uno de los más famosos y por ende uno de los más utilizados, especialmente en criptomonedas, en este algoritmo los nodos compiten por resolver un algoritmo matemático de alta complejidad que exige mucho poder computacional.
- Prueba de participación (PoS): este algoritmo de consenso se presenta como una alternativa a la prueba de trabajo y es usualmente empleada en *blockchains* públicas, a su vez es uno de los algoritmos de consenso más utilizados en *blockchain*, en este algoritmo de consenso los nodos que minan se les llama validadores, y la decisión sobre quién va a ser el nodo validador o el nodo que va a validar un bloque se hace de forma aleatoria, dando prioridad a los que cumplan con ciertos criterios (dependiendo del número de activos que posean), a diferencia de la prueba de trabajo este proceso es mucho más sencillo y no requiere tanto poder computacional, en este esquema de validación se premia a los usuarios que posean más reservas o activos.
- Prueba de participación delegada (DPoS): este tipo de consenso se deriva del PoS, ya que los propietarios de los criptoactivos eligen testigos, este tipo de consenso provee altos niveles de seguridad para uso en *blockchains* públicas, a su vez garantiza la escalabilidad. Una forma sencilla de entender este protocolo es la siguiente: los participantes de la red eligen delegados o testigos, una vez elegidos estos delegados, se les da la autoridad para producir y transmitir los bloques de transacciones dentro de la red, a diferencia del PoW en el que el sistema escoge el usuario con el mayor poder computacional, en este algoritmo el nodo delegado o el encargado de minar el bloque lo elige la misma comunidad que usa la red.
- Prueba de tiempo transcurrido (PoET): este algoritmo de consenso es altamente escalable y se enfoca en las *blockchains* privadas, la prueba de tiempo transcurrido crea un comité de confianza, en donde el comité o grupo de participantes son controlados por un controlador o administrador, este administrador tiene como su principal tarea el tomar el trabajo que han realizado las personas que integran el comité

de confianza y verificar que este es correcto, para ello el administrador o controlador comparte un tiempo que es aleatorio y una serie de pruebas criptográficas que habilita a los participantes aleatoriamente para que estos produzcan bloques dentro de la *blockchain*.

2.3. Características principales

Como se ha mencionado el *blockchain* es un sistema distribuido de libro contable, almacenado en una estructura similar a una cadena de bloques conectados, que contienen información validada y negociada colectivamente en una red punto a punto gracias a los algoritmos dedicados a tal fin. Las siguientes características principales y diferenciadoras de esta tecnología se logran gracias a la ayuda de algoritmos matemáticos y criptografía avanzada que proporciona un nivel de seguridad mayor a cualquier sistema de mantenimiento de registros descrito anteriormente [35].

2.3.1. Inmutabilidad de los datos

Cualquier nuevo bloque propuesto para la cadena tiene que hacer referencia a la versión anterior del libro mayor por medio del *hash* de identificación del bloque, los *hash* son bastante complejos y es imposible alterarlos y o revertirlos (obtener la información que contiene un documento partiendo del *hash*), esto crea una cadena de bloques que son inmutables dada la naturaleza de esta tecnología en la que los datos permanecen almacenados de forma cifrada o encriptada e irreversible, es así como la *blockchain* evita la manipulación, con la integridad de los registros, esta característica a su vez soporta la transparencia de los procesos. Si alguien quisiera corromper la red, debería modificar todos los datos almacenados en todos los nodos de la red, en redes que tienen millones de usuarios o nodos, acceder a estos nodos y hackearlos es casi imposible y necesita mucho poder computacional, además de su alto costo [35].

2.3.2. Trazabilidad

Esta es una de las características más importantes que tiene la tecnología *blockchain*, dada la inmutabilidad de los registros mencionados anteriormente y almacenamiento de todos los eventos registrados que dan la posibilidad de conocer todos los movimientos realizados de un elemento de información desde que este es registrado en la cadena de bloques, y así conocer los

Atributos asociados a este, como por ejemplo el momento y los actores que intervinieron en las transferencias de determinado elemento [35].

2.3.3. Verificabilidad

El libro mayor esta descentralizado, replicado y distribuido en múltiples ubicaciones que vendrían siendo los nodos de la red. Esto asegura alta disponibilidad ya que elimina un solo punto de falla, como pasa en los sistemas de datos centralizados, y también provee a los usuarios de un método seguro de verificación de la información, ya que todos los nodos de la red mantienen la última versión del libro mayor verificada por medio del consenso de la red, en la cual se encuentran almacenados todos los eventos que han tenido lugar en la cadena [35].

2.3.4. Consenso

Esta es una de las características más importantes del *blockchain*, se podría decir que las cadenas de bloques prosperan debido a estos algoritmos de consenso. Un algoritmo de consenso es el mecanismo usado por una red *blockchain* para seleccionar el estado correcto de un registro después de realizar una transacción, lo que indique el algoritmo de consenso se convierte en la verdad que todos los nodos deben seguir. Esto se hace normalmente seleccionando la mayoría de entre todos los estados propuestos. Bitcoin por ejemplo usa la prueba de trabajo o *Proof of Work* (PoW) en Inglés, en donde cualquier propuesta de estado del registro llega con el resultado de un cálculo complejo de *hash* que requiere bastante potencia de cálculo y se obtiene con la información consignada en el bloque que incluye entre otras cosas: los montos de las transacciones, las cuentas desde donde y hacia donde van las transacciones, *nonce*, marca de tiempo, entre otras cosas. La verificación de este cálculo es, sin embargo, bastante rápida y sencilla de verificar por los nodos mineros de la red. Por otra parte, el estado (que se trabaja por bloques de transacciones) tiene una referencia al estado anterior y al anterior por medio del *hash*, por lo que todos los bloques están enlazados y no es posible cambiar un bloque del pasado sin cambiar todos los siguientes, o por lo menos no con el poder computacional actual [31]. Cada red tiene su propio algoritmo de consenso para ayudar a la red a tomar decisiones, de esta manera los nodos pueden llegar a un acuerdo de forma sencilla y rápida, los nodos de la red pueden confiar en los algoritmos que se están ejecutando en su núcleo y esto da confianza a los usuarios de la red, ya que no deben confiar en los nodos

de la red, pero sí en sus algoritmos de consenso. Entre los algoritmos de consenso más usados en las cadenas de bloques se encuentran: prueba de trabajo (PoW), prueba de participación (PoS), prueba de participación delegada (DPoS), prueba de tiempo transcurrido (PoET), entre otras [35], [31].

2.3.5. Eliminación de intermediarios

Al ser una red par a par, las transacciones que suceden en la cadena de bloques son entre los participantes de la red, instituciones, grupos empresariales, empresas, personas, etc., estas pueden interactuar directamente entre sí, sin la necesidad de terceros de confianza como bancos o instituciones financieras, entre otras que validen y respalden las transacciones, eliminando así los sobrecostos y demoras asociadas a la intervención de estos terceros de confianza [35], [42].

2.4. Tipos de *blockchain*

2.4.1. *Blockchain* Pública

Una *blockchain* es llamada pública si todos los participantes tienen acceso a ella. En este tipo de *blockchain* no existe un ente central ni un tercero de confianza. Cabe decir también que este tipo de *blockchain* mantiene abiertos al público sus datos, software y desarrollo para que cualquier persona tenga la posibilidad de revisar, auditar y mejorar la misma [8].

- Las *blockchain* públicas permiten que cualquier usuario sea parte de ellas, ya sea como usuario, minero o administrador de un archivo de nodo, las personas pueden iniciar sesión en la red y ser parte de ella sin restricciones.
- El funcionamiento de la red es completamente transparente y abierto. Los datos de la cadena de bloques desde su creación están disponibles para todos sin restricciones. Cualquiera puede examinar o comprobar el funcionamiento de la red y su software.
- Cualquier persona puede revisar y auditar el funcionamiento de la red, así como auditar el código fuente.
- Este tipo de redes son descentralizadas, lo que significa que no existe un tercero de confianza o una autoridad central que regule el funcionamiento de la red.

- El mantenimiento económico de la *blockchain* depende de la minería y cobro de comisiones por cada una de las transacciones realizadas dentro de la red.



Figura 2.5. Blockchain publica.

2.4.2. *Blockchain Privada*

En las *blockchain* privadas ocurre al contrario de las redes públicas, estas dependen de un ente central que controla todas las acciones dentro de la red, como permisos dentro de la red ya sea para hacer transacciones, quién puede hacer transacciones, también el tipo de desarrollo es de tipo software privado, donde el ente central tiene que dar autorización para modificarla [8]. Algunas de las características de este tipo de *blockchain* son:

- El acceso a esta red está restringido por un ente central que decide quiénes pueden y qué pueden hacer dentro de la red.

- El acceso a la información que genera la red es restringido y privado.
- El mantenimiento económico, a diferencia de las *blockchain* públicas, recae sobre la entidad que sostenga la red, muy a menudo este tipo de redes no tienen su propia moneda ni operaciones de minería de bloques.



Figura 2.6. Blockchain privada.

2.4.3. *Blockchain* autorizada o híbrida

En una cadena de bloques autorizada algunos nodos se seleccionan previamente para participar en el proceso de transacción, en lugar de permitir a todos los participantes en una cadena de bloques pública o restringir el control a una sola entidad, organización o empresa como en una cadena de bloques privada. La velocidad de las transacciones y la eficiencia transaccional es sorprendente en una cadena de bloques autorizada, ya que los verificadores en este tipo de cadena de bloques son muy pocos, lo que reduce una gran cantidad de tiempo en el proceso de verificación. Una cadena

de bloques autorizada también garantiza que la privacidad de los datos del usuario esté garantizada, sin otorgar acceso completo a una sola entidad u organización [8].

Algunas de las características de este tipo de *blockchain* son:

- El acceso a esta red es a través de permisos que dependen del organismo que administra la red.
- Ciertos elementos dentro de la red son privados, dependiendo del criterio del administrador.
- Es flexible con respecto a las reglas de la red, sobre qué información es pública y que privada.

2.5. ¿Como funciona una *blockchain*?

De una manera muy sencilla, una *blockchain* sigue los siguientes pasos [34]:

- Nuevas transacciones o nuevos intercambios de información se transmiten a los nodos de la red.
- Cada nodo recolecta transacciones en un bloque.
- Cada nodo trabaja para encontrar la solución para la prueba de trabajo, que es un algoritmo con una dificultad alta para su bloque.
- Cuando un nodo encuentra la prueba de trabajo que funciona para su bloque, comparte el bloque a todos los nodos.
- Los demás nodos aceptan el bloque, solo si todas las transacciones dentro del bloque son válidas.
- Los nodos expresan su aceptación del bloque minado trabajando en la creación del siguiente bloque en la cadena, usando el *hash* del bloque aceptado como el *hash* anterior.

Los nodos siempre aceptaran la cadena más larga como la correcta y por ende seguirán trabajando con esta. Si dos bloques son minados al mismo tiempo, algunos nodos recibirán un bloque antes que otro por ende estos trabajarán con el primer nodo recibido pero guardaran la otra rama en caso de que esta se vuelva más larga. El empate se romperá cuando la siguiente

prueba de trabajo se encuentre y una rama se haga más larga que la otra, en este momento los nodos que estaban trabajando en la otra rama cambiarán a la más larga [34].

2.6. Inicios del *blockchain*

Esta tecnología nace en el año 1991 cuando Stuart Haber y W. Scott Stornetta, considerados por muchos como pioneros en esta área, describieron por primera vez un trabajo sobre cadena de bloques asegurados, el estudio que realizaron se llamó: Cómo sellar la hora en un documento digital, tiempo después presentaron un documento de complementación llamado: Mejorando la eficiencia y confiabilidad del sellado de tiempo digital [19], [9]. Estos dos, Haber y Stornetta, son por muchos considerados como los padres de la cadena de bloques, ya que su trabajo introdujo la idea de una cadena de bloques que usa *hash* o identificadores o sellos de identificación única, para crear un orden de compromisos para un conjunto de documentos en crecimiento constante, y a su vez estos dos artículos científicos son citados en el documento técnico de Bitcoin: Bitcoin: *A peer-to-peer electronic cash system*, escrito por Satoshi Nakamoto [34], documento al cual se debe en mayor parte la fama del *blockchain*.

Lo que expusieron Haber y Stornetta en sus trabajos fue lo siguiente: el sistema está compuesto por usuarios, un servicio de sello de tiempo (TSS - *time stamp service*) y un repositorio. En algún intervalo de tiempo el TSS publica un *Hash* “Intervalo”, el cual está disponible en un repositorio abierto y disponible a los usuarios. El proceso que describieron estos dos autores es el siguiente [19], [9]:

- Un usuario envía una solicitud de certificación al TSS.
- El servicio de sello de tiempo o TSS crea un árbol de Merkle de todas las solicitudes.
- El nuevo *hash* intervalo es calculado tomando el *hash* raíz del árbol de Merkle.
- El TSS publica el nuevo hash de intervalo en el repositorio público.
- El TSS envía a cada solicitante una prueba de Merkle de que su documento está comprometido en el árbol de Merkle.

- Los usuarios pueden validar la marca de tiempo de los documentos consultando el repositorio para el hash de intervalo relevante y usar la prueba de Merkle para comparar la hoja relevante con el *hash* del documento.

Pero esta tecnología se popularizó en realidad en 2008, como se menciona previamente, cuando un individuo o grupo bajo el seudónimo de Satoshi Nakamoto introdujo al mundo el protocolo Bitcoin y su software de referencia [34], un documento científico que describía un sistema *peer to peer* (P2P) o par a par de dinero digital, que se basa en una red descentralizada de ordenadores distribuidos por todo el mundo. Este documento técnico conectó el esquema de sellado de tiempo que habían propuesto Stornetta y Haber con la prueba de trabajo, en 2009 lanzó el software bitcoin y se crearon las primeras unidades de monedas que tomaron el nombre de Bitcoin. El propósito de la red Bitcoin era esencialmente eliminar el modelo de transacciones digitales basado en la confianza mediante la creación de una representación digital de dinero en efectivo. El estándar de pago electrónico hasta el 2008 que se publicó el documento de Satoshi Nakamoto siempre se hacía a través de instituciones financieras que aprueban y ejecutan cada transacción. Al crear un sistema de efectivo electrónico, se elimina la necesidad de confiar en proveedores externos. El objetivo se logró mediante la creación de un activo, Bitcoin, que permite transacciones entre pares que son inmutables y cifradas mediante criptografía para proteger a los usuarios del fraude.

2.7. Etapas de madurez de la tecnología *blockchain*

La idea de *blockchain* propuesta por Satoshi Nakamoto ha experimentado una rápida evolución con un crecimiento exponencial en los últimos años. Inicialmente, la tecnología no era programable, como con Bitcoin, pero han surgido tecnologías de *blockchain* que incorporan esta funcionalidad de programable. La idea de una cadena de bloques programable no necesariamente la hace mejor que una no programable, pero cumple una función específica y amplía en cuanto al alcance de la descentralización del mercado en un sentido general. Se pueden diferenciar las etapas del *blockchain* en 3 principales, expuestas brevemente a continuación.

2.7.1. *Blockchain 1.0*

La primera etapa de madurez de la *blockchain*, también denominada *blockchain 1.0*, está enfocada en transacciones, principalmente en el despliegue de criptomonedas y/o aplicaciones relacionadas con el efectivo, como transferencia de divisas y sistemas de pago digital. La idea detrás de *blockchain 1.0* era crear una nueva forma revolucionaria de abordar las finanzas. Con la introducción de un registro de transacciones en línea completamente descentralizado, distribuido e inmutable, *blockchain 1.0* tiene como objetivo brindar transparencia y acceso público al sistema financiero global. La introducción de Bitcoin en el año 2008-2009 como una solución de dinero digital basada en *blockchain* marcó el inicio de esta primera era. Esta es una etapa esencial del crecimiento de la tecnología *blockchain*, ya que, por primera vez en la historia financiera mundial, las transacciones monetarias se descentralizaron por completo, lo que significó que no hubo una sola empresa u organización que determinara las reglas del sistema. Esta primera etapa de esta tecnología poseía problemas de escalabilidad, con una capacidad de velocidad de procesamiento de transacciones de entre 3 y 7 transacciones por segundo, lo cual es muy poco si se compara con los volúmenes que pueden manejar los terceros de confianza tradicionales como Master Card, Visa, Paypal, entre otros; y pronto los desarrolladores como Vitalik Buterin atacaron este problema de escalabilidad y otros que tenía esta primera etapa, dando inicio a la *blockchain 2.0*.

2.7.2. *Blockchain 2.0*

En la *blockchain 2.0* el concepto y el enfoque cambian con respecto a la primer etapa del *blockchain*, ya que se evoluciona y se encuentran mejores prácticas y aplicaciones y se pasa de un concepto único de moneda digital a un esquema de contratos inteligentes, la introducción de contratos inteligentes da la posibilidad de realizar aplicaciones descentralizadas (Dapps), Organizaciones Autónomas Descentralizadas (DAOs), propiedad inteligente, tokens inteligentes, entre muchas más aplicaciones de esta segunda etapa del *blockchain*. Los contratos inteligentes, por su parte, son programas informáticos autónomos que se ejecutan de forma automática y en condiciones definidas de antemano. Estos contratos inteligentes se relacionan muy bien con *blockchain*, ya que gracias a las propiedades que ofrece el *blockchain*, hace que sea imposible manipular o hackear estos contratos. Por lo tanto, los contratos inteligentes reducen el costo de verificación, ejecución, auditoría y

prevención del fraude y permiten una definición transparente del contrato que supera el problema del riesgo moral sujeto a los humanos. El ejemplo más popular en esta etapa 2.0 del *blockchain* es Ethereum, cuyo objetivo es permitir la implementación de contratos inteligentes, es también muy importante mencionar que Ethereum fue la primera *blockchain* programable y más de un 70 % de las aplicaciones descentralizadas que existen hoy en día están programadas y operan sobre la red de Ethereum [29].

2.7.3. *Blockchain 3.0*

Blockchain 3.0 es una versión mejorada de *blockchain 2.0*, fue creada para mejorar las capacidades de la tecnología y resolver los problemas existentes, y al tiempo facilitar transacciones más rápidas, rentables y eficientes. Una de las cosas que hacen que *blockchain 3.0* sea notable y viable es DAG - *Directed acyclic graph* (Gráfico acíclico dirigido). Como su nombre lo indica, la información en una red basada en DAG fluye de forma acíclica, quiere decir que la información no se puede devolver al remitente. La información fluirá en una sola dirección. Se asegura de que los nodos no estén conectados a ninguno anterior. Tal estructura elimina los tiempos de bloqueo, que son 10 minutos para bitcoins y 20 segundos para Ethereum, que son los dos grandes ejemplos de la *blockchain 1.0* y la *2.0* respectivamente, lo que permite que las transacciones se procesen casi en tiempo real. DAG está siendo utilizado por la cadena IoT (ITC) y procesa 10.000 transacciones por segundo, mucho más que Visa, que procesa un poco más de 2.000 transacciones por segundo [29].

Capítulo 3

Sistemas de votación

3.1. El voto

El voto o sufragio es el mecanismo mediante el cual un individuo expresa su apoyo o preferencia por cierta opción, propuesta o candidato durante una elección. El voto es a su vez un método que sirve para medir la opinión conjunta de un grupo sobre alguna decisión que se quiera tomar de manera colectiva. El sufragio tiene como su implementación más popular el voto electoral y es parte esencial en todos los sistemas de gobierno que se basan en la democracia, ya que el voto es una condición necesaria para que un sistema político sea democrático.

3.2. Sistema de votación o sistema electoral

Un sistema de votación o un sistema electoral son un conjunto de reglas y procedimientos que regulan las distintas etapas de los procesos de votación, desde la forma en que se realizan las votaciones y cómo se determinan los resultados de las mismas. Un sistema de votación o sistema electoral define puntos clave, como las personas que están habilitadas para votar, las distintas formas de candidaturas, cómo se emiten los votos, el escrutinio de los votos, cómo se pueden realizar las campañas electorales, etc.

La votación y el conteo de votos son los principales eventos del proceso electoral. La votación es el medio por el cual los electores expresan su intención de voto para darle o no el apoyo a un representante u opción en específico y el conteo de votos significa la forma, el cómo, se cuenta y el peso que tiene cada voto. Existe una gran cantidad de variaciones en los sistemas electorales

Actuales, pero entre los sistemas más comunes se encuentran:

- Sistema de escrutinio mayoritario uninominal: el sistema electoral de escrutinio mayoritario uninominal es un sistema en el que el votante puede elegir un único candidato de entre los que se presentan, y el ganador será entonces el candidato que obtenga más votos.
- Sistema de segunda vuelta electoral: cuando en una elección ninguno de los candidatos supera un determinado porcentaje de los votos (por lo general el 50 por ciento + 1 voto), se realiza una segunda vuelta para decidir entre los candidatos que han obtenido más votos, usualmente los dos primeros.
- Escrutinio proporcional plurinominal: el sistema de escrutinio proporcional plurinominal es una categoría de sistemas electorales en la que el porcentaje de votos que reciben las candidaturas determina de manera proporcional el número de escaños que les son asignados en el órgano electo. Estos sistemas de representación se diferencian del escrutinio mayoritario uninominal porque las candidaturas no necesitan obtener mayoría relativa en ningún distrito electoral para poder ser representadas en el órgano elegido.

3.3. Principios fundamentales de los sistemas de votaciones democráticas

La democracia es el sistema político más utilizado ampliamente en el mundo, este sistema político tienen unas características básicas y necesarias para la democracia el incumplimiento de una sola de estas características significaría un sufragio no democrático. Estas características y requisitos son previos y universales, y por lo tanto independientes de la tecnología y procedimientos que se vayan a usar para realizar la votación. A continuación se mencionan los requisitos más importantes de una votación de elección y participación ciudadana:

- **Voto único:** el voto solo puede ser emitido por aquella persona que tenga el derecho a votar, y puede ser ejercido de forma efectiva solo una vez durante las votaciones. Esta condición se puede cumplir gracias al censo, el sistema de documentos de identificación y al sistema de colegios electorales.

3.4. *CONSIDERACIONES GENERALES DE UN SISTEMA DE VOTACIÓN*⁴³

- Voto privado: el voto tiene que ser totalmente secreto y nadie puede averiguar el voto emitido por un elector concreto.
- Integridad de los votos: una vez emitido, nadie debe ser capaz de cambiar los votos emitidos.
- Integridad de la votación: no puede ser posible que se modifiquen los resultados globales de la votación.
- Auditoría individual: Se debe asegurar que cada uno de los votos individuales se cuenten de manera correcta.
- Auditoría global: se debe garantizar que tanto el proceso electoral como el escrutinio de votos se desarrolle de manera adecuada cumpliendo con todas las garantías ya mencionadas.

El estudio de los métodos electorales definidos por cada nación se conoce como teoría de la elección social o teoría del voto, su campo de estudio se encuentra en el campo de la ciencia política, la economía o las matemáticas, y específicamente dentro de los subcampos de la teoría de juegos y el diseño de mecanismos.

3.4. Consideraciones generales de un sistema de votación

Los sistemas electorales requieren de ciertas acciones para garantizar su correcto funcionamiento, estas acciones reciben el nombre de operaciones electorales, a continuación una introducción de estas operaciones.

3.4.1. Registro de votantes

Este proceso en general es de los más complicados y costosos, ya que consume muchos recursos de logística y costos, a su vez es una de las tareas más importantes en la administración de elecciones. Este proceso, como lo indica su nombre, es aquel por el cual se establece quiénes son los individuos que pueden participar en cierta votación, este proceso de registrar votantes y generar las listas de los mismos en general toma más del 50 % del presupuesto dado. Son tres los sistemas principales para el registro de votantes, los cuales serán explicados brevemente a continuación:

- **Lista periódica:** la lista periódica es aquella lista que genera la respectiva autoridad electoral de cada elección en específico antes de cada elección, quiere decir que es cuando se genera una nueva lista de votantes habilitados para participar en el proceso electoral o de votación. Este tipo de listas se utilizan en general cuando el organismo electoral u organizador de la elección no tiene la infraestructura para mantener una lista permanente, también se usa cuando el ente electoral desea mantener una iniciativa de registro de electores antes de imponerles el registro en el mismo.
- **Registro continuo:** el registro continuo consiste en listas que se basan en registros de elecciones previas, con el objetivo de mantener una base de datos actualizada de los votantes. El registro continuo requiere de una inversión más alta con respecto a la lista periódica entre elecciones, ya que debe actualizar y mantener estas bases de datos. Pero los costos durante las elecciones son menores ya que al tener las bases de datos actualizadas permite una mayor agilidad en este proceso. El registro es utilizado en general cuando se realizan elecciones de manera constante y en muchas ocasiones existen alianzas entre las autoridades electorales y organizaciones que se encargan de actualizar regularmente las bases de datos, esto permite que exista una actualización en el registro electoral sin que haya un contacto directo entre las autoridades electorales y los electores.
- **Registro civil:** el registro civil es muy similar a un registro continuo. El registro civil está a cargo de una entidad o autoridad distinta a la autoridad de las elecciones y da a conocer con exactitud el estado civil de las personas y da entonces la legitimidad para ejercitar derechos públicos derivados de este estado civil, el voto, entre otros. En este tipo de registro la autoridad electoral tiene menos responsabilidades sobre las bases de datos de los electores, pero a su vez tiene menor control sobre las mismas.

3.4.2. Operaciones de voto

Las operaciones de voto son todas las actividades preparatorias que tienen lugar el día de las votaciones y su objetivo principal es el de garantizar que el día de las elecciones las actividades sean realizadas de manera organizada y eficiente para que las elecciones puedan ser fluidas, sistemas de

*3.4. CONSIDERACIONES GENERALES DE UN SISTEMA DE VOTACIÓN*⁴⁵

verificaciones de los electores que se presentan el día de las elecciones, métodos y herramientas para la emisión y escrutinio preciso del material resultado de las elecciones, personal calificado para apoyar a los votantes que requieran ayudas o tengan dudas sobre el proceso, privacidad de los electores, entre otras.

3.4.3. Identificación de los votantes

La identificación de los votantes es un proceso sumamente importante dentro de unas, ya que este proceso permite verificar la identidad de los votantes y tener un registro de las elecciones para evitar así que voten personas que no están habilitadas para votar y evitar que las personas voten más de una vez. En la mayoría de las elecciones la manera como se realiza la identificación de los votantes es mediante el documento de identidad de los votantes, en donde el votante comprueba que es el titular del documento y a su vez se comprueba su estado de habilitado o no para votar.

3.4.4. Escrutinio

El escrutinio de los votos es un proceso fundamental dentro de las elecciones, es un proceso que se hace al finalizar las elecciones y que consiste en el conteo de los votos de un proceso de votación. Depende de cada ente electoral garantizar que todos los votos se cuenten de manera precisa y transparente. El proceso de escrutinio de votos debería hacerse en presencia de los partidos políticos, representantes o candidatos y observadores del proceso.

Este proceso es uno de los más importantes, pero a su vez es uno de los más controversiales, ya que está expuesto a mucha corrupción y si no se hace un escrutinio correcto esto puede significar la pérdida de confianza de los electores.

3.4.5. Auditorías

Las auditorías dentro del proceso electoral se utilizan para proteger la integridad y transparencia de las elecciones. Este proceso se encarga de vigilar el correcto funcionamiento de todo el proceso electoral. Generalmente, en este proceso de auditoría participan expertos en el área, los cuales analizan todo el proceso electoral en general.

3.5. Breve historia del sufragio universal

El sufragio universal se ha vuelto una norma en la mayor parte del mundo, gracias a la democracia se ha incrementado la participación pública en asunto de toma de decisiones y asuntos políticos, la democracia tiene como su mayor argumento la participación de las masas en elecciones democráticas y la relación que existe entre electores, candidatos y estructuras políticas. Las asambleas de la antigua Grecia y Roma fueron las primeras que realizaron elecciones de manera muy rudimentaria y con muchas restricciones, en donde solo una parte de la población tenía acceso a este derecho. Luego, durante gran parte de la Edad Media, las elecciones surgieron en las asambleas locales y regionales. Sin embargo, las elecciones, tal como se han venido desarrollando en la Edad Moderna, fueron establecidas en Europa con la Revolución Francesa, donde se pasó de una monarquía absolutista, en ella tenían el poder total la nobleza y la iglesia católica, a una república en la que ya no existían súbditos y se reconoció a cada persona como ciudadano. Uno de los grandes avances que trajo la Revolución Francesa fue la definición de una constitución, la cual establece que la soberanía reside en la nación y no en el rey, como venía siendo la norma hasta ese entonces, y de una asamblea de representantes en donde los ciudadanos hombres y con una situación económica estable tenían derecho a ser un posible candidato y el derecho a escoger sus diputados, los cuales tendrían la responsabilidad de velar por sus derechos e intereses ante los altos mandos del estado; lo mismo sucedía en los Estados Unidos, siendo estos dos los primeros antecedentes de la Edad Moderna en cuanto a temas de parlamentos democráticos; por esto siempre que se habla de la historia del voto y de los derechos del ciudadano hay que nombrar estos dos sucesos, los cuales cambiaron el curso del mundo y terminaron con el antiguo régimen.

Las elecciones modernas son definidas por algunos como la base para selección de asambleas parlamentarias enfocadas en el ciudadano como unidad electoral y a su vez el mecanismo para alcanzar un consenso de los electores y quienes los gobiernan [27]. De aquí el concepto de gobierno representativo basado en el principio de: un individuo un voto. Estos principios no fueron cumplidos siempre, ya que hasta el siglo XIX en los Estados Unidos y la gran mayoría de países europeos, el voto o sufragio era un derecho que tenían ciertas personas de la sociedad, que desempeñaban un papel fundamental en la sociedad, eran reconocidos como honorables miembros de la misma, eran adinerados o tenían cercanía con los que tenían el poder en ese momento [17]. En el siglo XIX las tantas revueltas populares que sucedían en Europa generaron

un cambio de control de las monarquías a las asambleas populares, esto produjo que el sufragio fuera reconocido a los hombres que cumplieran con ciertas condiciones como el número de propiedades que tuvieran a su nombre o el nivel de ingresos.

Aunque se había avanzado mucho en el tema del sufragio este seguía en manos de una pequeña elite de la población, además de ciertas incoherencias e injusticias con respecto a votos múltiples dependiendo del nivel de riqueza y estatus en la sociedad o parámetros para determinar el conteo de votos. Todo esto cambió a finales del siglo XIX, ya que estos criterios sociales y económicos de la elite fueron abolidos gracias a los movimientos revolucionarios y la industrialización, que fueron una combinación perfecta para la organización y rebelión de la clase obrera, como resultado a estos sucesos la mayoría de hombres mayores de edad obtuvieron el derecho al voto en Europa y Estados Unidos. El sufragio femenino es otra historia, ya que las mujeres, siendo más de la mitad de la población del mundo, no han tenido derechos políticos, no han tenido el derecho a elegir ni ser elegidas durante mucho tiempo y apenas pudieron acceder a este derecho solo a finales del siglo XIX y principios del siglo XX. El primer país que aprobó el sufragio femenino fue Estados Unidos (1869), Nueva Zelanda (1893) siguió sus pasos y aprobó el primer sufragio femenino en este país, aunque las mujeres podían votar, no podría asistir a las elecciones y debían enviar el voto por correo y el sur de Australia (1895) a diferencia de Nueva Zelanda, Australia habilitó el voto femenino pero además permitió la asistencia de las mujeres a los puestos de votación. Otros países como Finlandia, Noruega, Dinamarca y Suecia, habilitaron el sufragio femenino entre 1906 y 1921. Muchos países europeos como Francia, Bélgica e Italia no reconocieron el sufragio femenino hasta después de la Segunda Guerra Mundial, en Colombia, por ejemplo, el voto femenino fue aprobado apenas en el año 1954, en la dictadura de Gustavo Rojas Pinilla. Cabe mencionar que en algunos países del mundo el voto femenino no ha sido reconocido aún o tiene requisitos para que las mujeres puedan acceder al voto, entre ellos Libano, Afganistán, Kuwait y Arabia Saudita, que no permiten que las mujeres voten.

Capítulo 4

Sistemas de Votaciones Electrónicas

4.1. Sistemas de Votaciones Electrónicas

El término voto electrónico incluye todos los métodos que permiten la emisión y conteo de votos a través de tecnologías electrónicas o informáticas, existen varios tipos de sistemas para las votaciones electrónicas. Los principales sistemas de votaciones electrónicas incluyen: sistemas con tarjetas perforadas, registro electrónico directo RED, registro electrónico directo RED en red pública y votación por internet.

El voto electrónico tiene la capacidad de convertirse en la forma más rápida, barata y eficiente de administrar las elecciones y contar los votos, ya que consiste en un proceso o procedimiento simple y requiere pocos trabajadores dentro del proceso. Estos sistemas de votación electrónicos a su vez se pueden dividir en dos principales grupos: votaciones en sitio y votaciones remotas. El sistema de votación electrónica en el sitio es cuando los votantes son identificados a través de su tarjeta de identidad en puntos de votación designados, pero utilizan maquinas en un dispositivo electrónico en lugar del formulario tradicional en papel, de esta manera, con este tipo de votación electrónica los ciudadanos necesitan movilizarse a las estaciones o puntos electorales designados donde pueden encontrar los dispositivos electrónicos. El otro tipo es el proceso de votación a distancia o remoto, a través de este sistema los votantes pueden optar por votar mediante el uso de dispositivos móviles con acceso a internet desde cualquier ubicación. En este tipo de votación electrónica, tanto las computadoras como el internet, se utilizan para votar a través de una aplicación o software, donde los votantes siguen

los mismos pasos que los votantes en el lugar, pero de forma remota mediante internet, lo que reduce el costo de la movilidad, entre otros costos que se reducen en este proceso.

4.1.1. Sistema de tarjetas perforadas

En estos sistemas de tarjetas perforadas los votantes perforan sus tarjeta para indicar su voto, después esta tarjeta se introduce en una computadora con un mecanismo de tabulación especial. Se utilizaron por primera vez en Estados Unidos en las elecciones presidenciales de 1964.

4.1.2. Registro Electrónico Directo RED

Las máquinas de votación de registro electrónico directo son máquinas que presentan el tarjetón a los votantes de forma electrónica, el votante puede interactuar con estas máquinas mediante una pantalla táctil o por medio de botones, como en los cajeros automáticos, para emitir su voto, una vez realizado el voto, este será almacenado dentro de la memoria de esta máquina.

La máquina de registro electrónico directo realiza una tabulación veloz de los datos, la cual es almacenada en la memoria interna de la misma. Una vez finalizadas las elecciones la información de todas las maquinas RED, se recopilan en computadoras centrales, las cuales se encargan de validar y calcular los resultados finales.

Los sistemas basados en máquinas RED tienen muchos beneficios, como el conteo de los votos de una manera mucho más rápida y el ahorro de dinero con la no impresión de los tarjetones de papel, pero tiene aún muchos asuntos pendientes en temas de seguridad.

Una variación que tienen estos sistemas, es su implementación conjunta con el internet como medio para transmitir los votos a una maquina o servidor específico. Las dos variantes de este RED tienen altos niveles de inseguridad con respecto a la transparencia del proceso y vulnerabilidad de los datos.

4.1.3. Votaciones por Internet

Las votaciones por internet o *i-voting* como su nombre lo indica, son sistemas que se utilizan a través de un dispositivo con acceso a internet. Estonia es el ejemplo más emblemático de las votaciones por internet, en donde los ciudadanos con la tarjeta de identidad se les permite votar desde internet.

El sistema tiene una infraestructura de llave pública para garantizar la seguridad y privacidad del proceso, pero este sistema tiene también muchas alertas y muchas fallas en cuanto a la transparencia de los procesos y la vulnerabilidad de los datos.

4.2. Ejemplos de voto electrónico en el mundo

Estonia fue el primer país en implementar una votación electrónica en 2007, permitiéndole a los ciudadanos emitir su voto de forma remota a través del internet gracias a su tarjeta de identificación nacional electrónica [7], cabe mencionar que es el único país en el mundo actualmente que permite el uso de votaciones por medio de internet para elecciones oficiales. La tarjeta de identificación utilizada permite la autenticación y la firma electrónica encriptada usando los algoritmos de *hash* seguros SHA1 / SHA2 [7]. La tarjeta de identificación de Estonia también permite el acceso a otros servicios electrónicos de Estonia como cuentas bancarias, seguro médico y prueba de identidad cuando se viaja dentro de la UE. La tarjeta de identificación utilizada en las elecciones se diseñó para funcionar en un circuito integrado, una plataforma de chip Java y protegido con un PIN de 2048 bits [7]. La tarjeta es fácilmente utilizable para autenticación, cifrado y firmas. El votante tiene que descargar la aplicación para votar designada por el gobierno de Estonia, también se tiene que autenticar usando la identificación electrónica, y si el votante está habilitado para votar, se mostrará una lista de candidatos y se podrá emitir un voto. El voto se cifrará con la clave pública de la elección y se firmará con la clave privada del votante. Tan pronto como se emite el voto este es enviado a un servidor de almacenamiento de votos controlado por el gobierno de Estonia. Los votantes pueden votar varias veces y solo se considerará válida la última votación. Esto se hace para evitar la compra de votos.

Noruega, en el año 2011 y 2013, utilizó un sistema electrónico de voto a distancia para las elecciones parlamentarias. El sistema fue desarrollado por el proveedor de votación electrónica Scytl y era muy similar al sistema de votación electrónica de Estonia. Sin embargo, en 2014 el país suspendió su proyecto de *i-vote* debido a preocupaciones de seguridad. Una de las principales críticas que enfrentó el sistema de *i-voting* noruego fue el temor a que en caso de un cyberataque los votos se hicieran públicos [15].

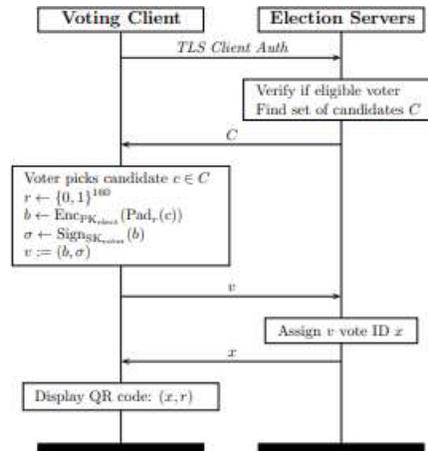


Figura 4.1. Modelo emisión de votos *i-voting* Estonia [41].

Una de las principales críticas que tienen estos sistemas de votaciones, tanto el de Estonia como el de Noruega, es que hay partes del código fuente que son fundamentales pero a su vez secretas. También la publicación de los resultados de la votación en el sistema *I-Voting* de Estonia se hace a puerta cerrada, lo que genera dudas sobre la transparencia del proceso. Un sistema de votación electrónica de código abierto es imprescindible para una elección confiable y transparente.

En **Canadá**, las elecciones federales y provinciales son realizadas mediante tarjetones de papel, sin embargo, desde los años noventa el voto electrónico es posible para las elecciones a nivel municipal.

Brasil fue de los primeros países que implementaron el voto electrónico desde el año 1996, actualmente el voto electrónico está habilitado para elecciones presidenciales, Brasil utiliza un método basado en máquinas de votación electrónica de grabación directa DRE (*voting machine* en inglés). Estas máquinas realizan la identificación del votante, el proceso de emisión del voto y el almacenamiento del mismo en un solo proceso, además de la incorporación de identificación biométrica desde el año 2012. Este sistema ha sido muy criticado ya que carece de procesos de auditoría, no se generan comprobantes o recibos para que el votante pueda verificar su voto, no se protege la anonimidad del voto al otorgar listas de votantes con identificación personal e información de su votación, entre muchas otras críticas que tiene este sistema.

4.3. Sistemas de votaciones basados en tecnología *blockchain* BVS

Los sistemas de votaciones basados en tecnología *blockchain* (BVS por sus siglas en inglés) han sido ampliamente estudiados en los últimos años. Esto se debe principalmente a las propiedades de esta tecnología como la imposibilidad de modificar los datos una vez almacenados y la eliminación de terceros de confianza para la revisión de los datos emitidos y almacenados [34]. Este tipo de investigaciones tienen diversos enfoques que van desde el impacto económico que generarían unas elecciones 100 por ciento confiables y seguras de manera electrónica [4], [37], hasta enfoques que cuestionan la reorganización completa de la sociedad a través de la modificación profunda de las instituciones estatales [6]. Partiendo de la comprensión de la tecnología *blockchain* como un agente altamente disruptivo en la sociedad, que permite el desmonte de todos los procesos burocráticos, reemplazándolos por él “*Blockchain Government*” [23], un interesante concepto que se basa en cinco principios fundamentales:

1. Introducción del estatuto de ley *blockchain*. Creación de las leyes necesarias para la instauración de un gobierno basado en *blockchain*.

2. Transparencia en la revelación de los datos y el código fuente.

Posibilidad de ver toda la trazabilidad de los datos almacenados en la *blockchain* gubernamental, la cual debe ser implementada con estándares de código abierto para permitir las auditorías al código por parte de cualquier ciudadano.

3. Implementación de una administración ejecutiva autónoma.

Modificar los procesos burocráticos, para ejecutar estas funciones directamente sobre la *blockchain* estatal. Ejemplo: registros de nacimiento y defunción; conectando los hospitales a la *blockchain* del estado, los partes médicos generan automáticamente los respectivos registros cuando un bebé nace, o cuando una persona muere.

4. Construcción de un sistema de gobierno basado en democracia directa.

Los ciudadanos toman decisiones más complejas sobre el estado, permitiendo reducir considerablemente el número de congresistas y senadores, y generando la posibilidad de que sean los ciudadanos los que voten por la aprobación o derogación de los proyectos de ley.

5. Construir un Gobierno Distribuido Autónomo (DAG).

La suma de los cuatro puntos anteriores lleva a la creación de un Gobierno Distribuido Autónomo, DAG por sus siglas en inglés. En donde se reduce la burocracia y se incrementa exponencialmente la eficiencia del estado.

Esta tecnología es muy novedosa y tiene mucho potencial para ser un agente disruptor en nuestra sociedad si se adopta como base para todos los procesos del estado y en general procesos que requieran una precisión y transparencia que garantice así la integridad y las necesidades de los usuarios en función de un bien común. También existen variables y situaciones que hacen del *blockchain* una área muy peligrosa si no define bien la participación y los protocolos de consenso para cada una de las redes, que garanticen la transparencia y efectividad de los procesos que adopten como base *blockchain*. En [30], se advierte de los cuidados que se debe tener al implementar esta tecnología, puesto que un mal uso de la misma puede resultar en problemas de inequidad, falta de transparencia y debilitamiento de la democracia. Por eso muestran cómo se puede evitar llegar a estos escenarios a través de la identificación de tendencias clave.

La implementación de un sistema de votación basado en tecnología *blockchain* puede sonar descabellado y muy lejos de la realidad debido al conflicto de intereses que existe en esta área, sin embargo, en los países desarrollados estas posibilidades se están comenzando a explorar seriamente [23], [6], [10]. En Estonia, por ejemplo, se ha avanzado mucho en temas de democracia directa y elecciones basadas en internet y *blockchain*. En China están creando una *blockchain* estatal para agilizar los trámites y eliminar la burocracia. Por otro lado, el Foro Económico Mundial está impulsando la adopción masiva de soluciones de *blockchain* estatales en los países aliados a dicho foro. En el campo específico de las elecciones basadas en *blockchain*, se ha demostrado que este tipo de implementaciones generan una mayor confianza en el elector, ya que permiten erradicar el principal problema de los sistemas de votación actuales, el cual es la posibilidad de fraude, entre otros factores [11]. Lo anterior es muy importante, ya que las sociedades están experimentando una “erosión de la confianza en el principal pilar de la democracia, el sistema de elecciones y votaciones” [39], dicha confianza puede ser restaurada con la implementación de la tecnología *blockchain* en los sistemas sociales.

Además de los problemas de confianza que impactan a las elecciones, en [38] plantean un escenario en el cual los ciudadanos pueden informarse de la gestión que un gobernante realiza sobre un territorio, desplegando una red de dispositivos conectados a la red, que censan constantemente diversos

4.3. SISTEMAS DE VOTACIONES BASADOS EN TECNOLOGÍA BLOCKCHAIN BVS55

parámetros como la calidad del agua, el aire, el flujo del tráfico. Estos datos se escriben en una *blockchain* estatal, para su posterior consulta, y así poder medir la gestión realizada por el gobierno local por parte de los ciudadanos, para que luego se pueda emitir un voto más informado.

Lo países del primer mundo no están ajenos a la falta de confianza en su sistema de votaciones. En Estados Unidos, para el año 2016, hubo serios rumores de que el sistema de voto electrónico fue vulnerado por hackers extranjeros, rusos para ser más exactos [32]. En [32] exponen la necesidad de migrar el voto electrónico a uno basado en *blockchain* para evitar la manipulación e incrementar la confianza de los votantes.

En [22] profundizan en el diseño de un sistema de votaciones basado en *blockchain*, generando los siete requerimientos mínimos que debe tener todo sistema de votaciones que utilice esta tecnología:

- No se pueden permitir votaciones coercionadas.
- Se debe permitir un método para asegurar la autenticación segura a través de un servicio de verificación de identidad
- No se debe permitir el rastreo del voto para saber quién votó por quién.
- Se debe proveer la transparencia necesaria para que cada votante pueda verificar que su voto fue contado correctamente y sin que esto suponga un riesgo a la privacidad del votante.
- Se debe evitar que cualquier tercero pueda alterar el voto emitido.
- No se debe permitir a una sola entidad determinar los resultados de las votaciones (el resultado es el que emita la *blockchain* y no una entidad).
- Solo se debe permitir que los individuos elegibles puedan votar.

Sumado a lo anterior, en [13] exponen los procedimientos necesarios para llevar a cabo unas elecciones populares de manera exitosa, utilizando *blockchain*. Además, introducen los conceptos necesarios para habilitar a los votantes, para emitir su voto desde sus dispositivos móviles, apeándose a los principios expuestos en [22].

En [24] proponen una arquitectura por capas detallada de un sistema de votaciones basado en *blockchain*, utilizando una *blockchain* llamada *multi-chain*. También hacen un importante énfasis en cómo a través de los mecanismos implementados en *blockchain* para evitar el doble gasto, sirven

perfectamente para que en un sistema de votaciones se elimine la posibilidad de doble voto.

Sin embargo, no todo son propuestas o proyectos, en [23] muestran experimentos llevados a cabo a principios del año 2018 por parte de una empresa llamada Voatz, la cual realizó pruebas en los Estados Unidos de votaciones con *blockchain* a través de teléfonos móviles en grupos de iglesias, gobierno escolar, organizaciones sin ánimo de lucro, sindicatos, reuniones del consejo de la ciudad de Massachusetts y eventos de partidos políticos subnacionales. Todo lo anterior, se asienta sobre una base fundamental: los EVS (*Electronic Voting Systems*), estos sistemas de voto electrónico se han venido desarrollando desde los años setenta [24], y su evolución apenas natural son los EVS basados en *blockchain*. En [5] explican, entre otras cosas, los principios de todo EVS, los cuales se resumen en: Generalidad, Libertad, Equidad, Secreto, Franqueza y Democracia. Todos los intentos de incrementar la confianza de los electores a través de sistemas de votación electrónicos han fallado, puesto que a pesar de contar con interfaces electrónicas para realizar el voto, los datos están centralizados y no se permiten las auditorías por parte de cualquier ciudadano. En [37] muestran cómo la única forma de devolverle la confianza a los electores es a través la utilización de las ABVS (*Auditable Blockchain Voting System*).

Como se dijo, la evolución de los EVS son los sistemas basados en *blockchain*, en [26] se este concepto a las ABVS (*Auditable Blockchain Voting System*). Los ABVS (*Auditable Blockchain Voting System*) tienen grandes ventajas, siendo una de las más importantes, la posibilidad de poder votar a través de internet de manera anónima y segura, con la posibilidad de que cualquier integrante de la red, puede verificar la información allí depositada. Estos sistemas tienen unos componentes específicos descritos a continuación [2]:

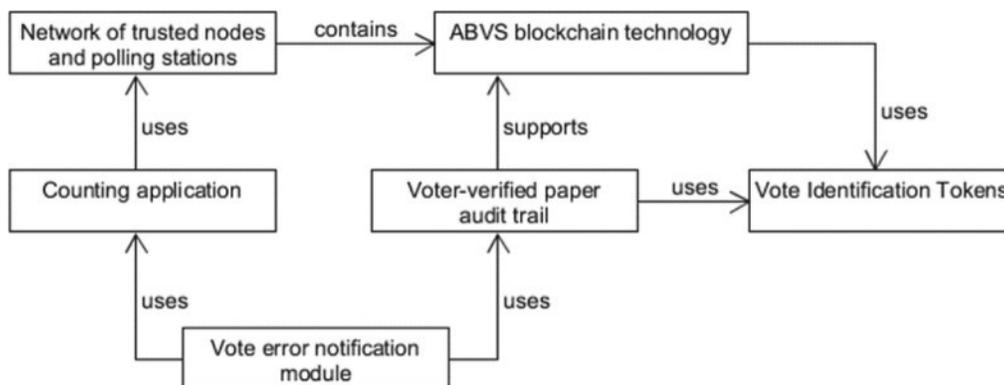


Figura 4.2. Esquema de relaciones entre componentes de un ABVS [2].

4.3. SISTEMAS DE VOTACIONES BASADOS EN TECNOLOGÍA BLOCKCHAIN BVS57

- *Network of trusted nodes and polling stations* (Red de nodos y centros de votación de confianza): consiste en dos partes, la primera de ellas es un supernodo de confianza, que representa a la autoridad nacional electoral (Registraduría Nacional del Estado Civil), los demás nodos son instituciones públicas preseleccionadas y verificadas, por ejemplo, universidades. Todos los nodos agregaran poder de procesamiento y se encargará de almacenar una copia de todas las elecciones almacenadas en la ABVS. Además, serán responsables de la verificación de las transacciones y toda la *blockchain*. La segunda parte está compuesta por las estaciones de votación, entendidas como el hardware y software del ABVS asociados con la ubicación de las estaciones de votación. Los votantes las usan para emitir su voto, el cual será transmitido a los nodos para su verificación y procesamiento en concordancia con el paradigma de las estructuras de datos *blockchain*.

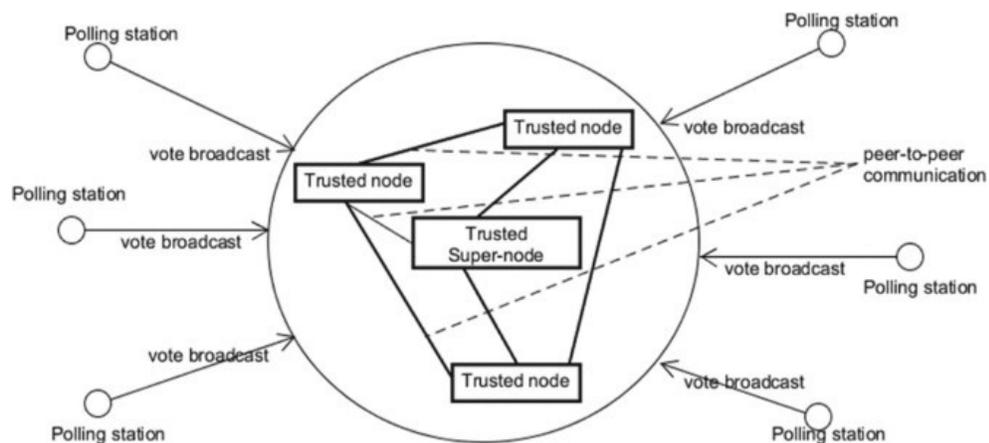


Figura 4.3. Esquema de red ABVS [2].

- *Vote Identification Tokens* (VITs) (Fichas de Identificación del Voto): son códigos alfanuméricos los cuales son utilizados como medios de autenticación y autorización de los votantes dentro del sistema. Los VITs permiten además el seguimiento del voto durante y después de las elecciones. Se pueden almacenar en tarjetas raspables, hojas de papel en sobres sellados o cualquier otro medio que permita una selección aleatoria de los VITs por parte de los votantes sin que sepan su contenido previamente. Los VITs son creados antes de las elecciones y son asignados y distribuidos entre las estaciones de votación. Una base

de datos con los VITs asignados a cada estación se mantiene en los nodos de confianza. La tecnología *blockchain* es el núcleo de todo el sistema. Particularmente, para los ABVS existe una excepción con el paradigma *blockchain*: los nodos que verifican y procesan nuevos votos (transacciones), están restringidos solo a instituciones públicas verificadas y certificadas, y no es cualquier persona con voluntad de participar en la red. La estructura de datos de un ABVS está hecha de bloques que almacenan las transacciones con la información descrita en la siguiente figura:

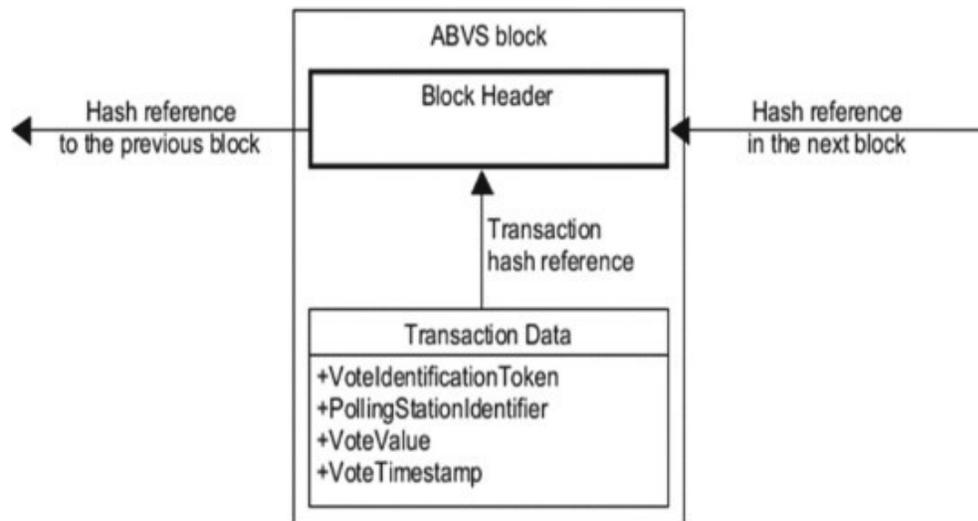


Figura 4.4. Modelo de bloques de red ABVS [2].

- *Counting application* (Aplicación de conteo): es una aplicación firmada y verificada, cuya tarea es iterar sobre la *blockchain* ABVS y contar los votos. Con el fin de proveer tolerancia a los fallos, cada nodo de la red ABVS está equipado con su propia copia de la app.
- *Voter-verified paper audit trail* (VVPAT) (Seguimiento de auditoría en papel verificado por el votante): es un ticket de papel que contiene la misma información que un bloque como el de la figura 3. Estos tickets se imprimen cuando el ciudadano emite su voto y son almacenados en una urna física dispuesta en el sitio de votación. Eso le brinda a la ABVS un sistema extra para auditar las elecciones. Se asume que los

4.3. SISTEMAS DE VOTACIONES BASADOS EN TECNOLOGÍA BLOCKCHAIN BVS59

VVPATs toman precedencia sobre el contenido de la *blockchain* en caso de presentarse inconsistencias.

- *Vote error notification module* (Módulo de notificación de errores del voto): es una aplicación dedicada a notificar los posibles errores. El votante que encuentre inconsistencias con su voto puede, anónimamente, notificar a los encargados de las elecciones proporcionando su VTI y la explicación del error. Las quejas interpuestas por VITs válidos son procesadas.

El principal beneficio de los sistemas ABVS es la posibilidad de verificar de extremo a extremo gracias al uso de la tecnología *blockchain*. Los votantes están en capacidad de seguir y controlar sus votos y, gracias a los VITs, los VVPATs y el reporte de errores con el voto permanecen anónimos. Cumpliendo de esta manera con los principios y requerimientos mínimos de las elecciones.

Capítulo 5

Descripción de la propuesta

En este capítulo se exponen las propiedades que fueron tenidas en cuenta y se utilizaron como base para el diseño e implementación del modelo de votación propuesto, utilizando la tecnología *blockchain*, así como los requerimientos no funcionales del software, los cuales fueron tenidos en cuenta para el diseño de la *blockchain*. Todo esto se hizo para que los usuarios de esta herramienta tengan las garantías mínimas que un proceso tan delicado como el proceso de votación debe tener.

5.1. Propiedades del sistema propuesto

5.1.1. Imparcialidad

En las elecciones, y en general en los sistemas de votaciones, los resultados parciales de las elecciones no pueden ser públicos si las elecciones no se han finalizado aún. El escrutinio parcial y el total de los votos solo podrá ser posible hasta finalizar las elecciones para evitar que se perjudiquen ciertas organizaciones o candidatos y no se den ventajas a los candidatos u opciones que lleven o no la delantera en las elecciones, creando un sesgo por el hecho de saber el estado actual de las elecciones. Para lograr esto, el sistema propuesto solo correrá el algoritmo de conteo de los votos cuando la hora y fecha actual sea mayor a la fecha y hora de finalización de la elección. Parámetro que se ingresa al momento de crear una nueva elección en el sistema.

5.1.2. Privacidad

La privacidad se refiere a la propiedad de los sistemas de votaciones, la cual mantiene en secreto tanto la información de los votantes como el contenido de su voto. Este es uno de los puntos más fuertes que tienen las votaciones usando tecnología *blockchain*, ya que la identidad de los votantes va a estar enmascarada por un par de llaves criptográficas y de igual manera va a ser privado el voto que el usuario deposite en la *blockchain*, esto para evitar repercusiones que podrían existir si la identidad de los usuarios y su preferencia u opción seleccionada son públicas.

La política de tratamiento de datos se define de conformidad con la entrada en vigencia de la Ley Estatutaria 1581 de 2012, la cual tiene por objeto “dictar las disposiciones generales para la protección de datos personales y desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos así como el derecho a la información”.

5.1.3. Verificabilidad

La verificabilidad del sistema es la capacidad que tiene cada uno de los votantes para verificar que su voto fue almacenado de manera correcta para la opción que acabó de seleccionar, en nuestro prototipo al finalizar cada elección el usuario recibe un certificado de votación con el *hash* que localiza su voto, el cual después puede ser verificado en la red *blockchain* para ver la localización de su voto, de esta manera los votantes podrán rastrear y verificar que su voto fue contado de manera correcta.

5.1.4. Auditoría

La auditoría es la capacidad de examinar todo el proceso de elecciones para verificar la transparencia y/o integridad de las mismas. Al ser una propuesta o un prototipo que se basa en el software libre, las auditorías están abiertas al público para que verifiquen la integridad y el diseño del software y la red *blockchain* para garantizar unas elecciones transparentes de inicio a fin.

5.1.5. Resistencia a la coerción

La coerción se puede definir como la acción mediante la cual se ejerce presión a un individuo o con el objetivo de condicionar su comportamiento,

en este caso preciso de votaciones para condicionar su elección. Con esta solución se puede brindar a los votantes una seguridad y tranquilidad para efectuar su voto sin presiones, ya que su decisión es privada y puede tener la certeza que su identidad y elección van a estar en el anonimato para agentes externos a la votación, incluso para los administradores de la *blockchain*.

5.1.6. Usabilidad

La usabilidad se refiere a las condiciones que facilitan el proceso de votación por parte de todos los participantes de la red de votación desde los organizadores hasta los votantes. Usabilidad también incluye las facilidades que dispone el sistema para facilitar la votación, esto es un punto fundamental ya que la facilidad para acceder al sistema de votación puede incrementar drásticamente el número de personas que participan en las mismas. La herramienta cuenta con una interfaz de usuario fácil de manejar, intuitiva y sencilla; además de las comodidades conocidas del internet que permiten que los usuarios participen de las elecciones desde cualquier dispositivo móvil con acceso a internet.

5.2. Requerimientos no funcionales

Los requerimientos no-funcionales son muy importantes, aunque en muchos casos ignorados en las fases de creación de un sistema, estos requerimientos son criterios que se deben cumplir para un correcto funcionamiento y para que los sistemas puedan tener un uso adecuado. Para el caso de estudio que se está realizando de un sistema de votaciones basado en la tecnología *blockchain*, pudimos analizar e identificar los siguientes requerimientos no funcionales:

- Tolerancia a fallos
- Rendimiento
- Escalabilidad
- Descentralización
- Portabilidad
- Seguridad

- Disponibilidad
- Transparencia

5.3. *Stack* utilizado

El *stack* utilizado para desarrollar este proyecto de diseño de un sistema de votación electrónica usando *blockchain* fue el siguiente: para el *backend* se utiliza NodeJS con el *framework express*. Para la *blockchain* se utiliza *Multichain* con dos nodos. La interacción con la *blockchain* se hace a través de la librería de *Multichain* para NodeJS. En el *frontend* se utiliza Ionic con Angular.

Capítulo 6

Arquitectura de software

El modelo de vistas de arquitectura 4+1 describe la arquitectura de sistemas del software propuesto, este modelo de vistas consiste en el uso de múltiples vistas concurrentes para describir el software desde distintos puntos de vista, están enfocados en cada una de las diferentes partes interesadas del proyecto, entre los cuales podemos encontrar los siguientes: usuarios finales del software, programadores, administradores del proyecto, entre otros. Cada punto de vista de una arquitectura representa un subconjunto de componentes que interactúan entre sí, provenientes de una o varias estructuras con una función o significado particular dentro del sistema. En el modelo se proponen cuatro vistas principales: vista lógica, vista de desarrollo, vista física y vista de procesos, y una vista adicional utilizada para unir las otras que es la vista de escenarios o casos de uso que se utiliza para validar el diseño de la arquitectura [25].

6.1. Vista de desarrollo - Modelo entidad-relación

Los diagramas entidad-relación (diagramas ER) muestran el diseño conceptual de aplicaciones de bases de datos. Describen las distintas entidades del sistema de información y las relaciones y restricciones existentes entre ellos. Es un tipo de diagrama de flujo que ilustra cómo las entidades, como personas, objetos o conceptos, se relacionan entre sí dentro de un sistema.

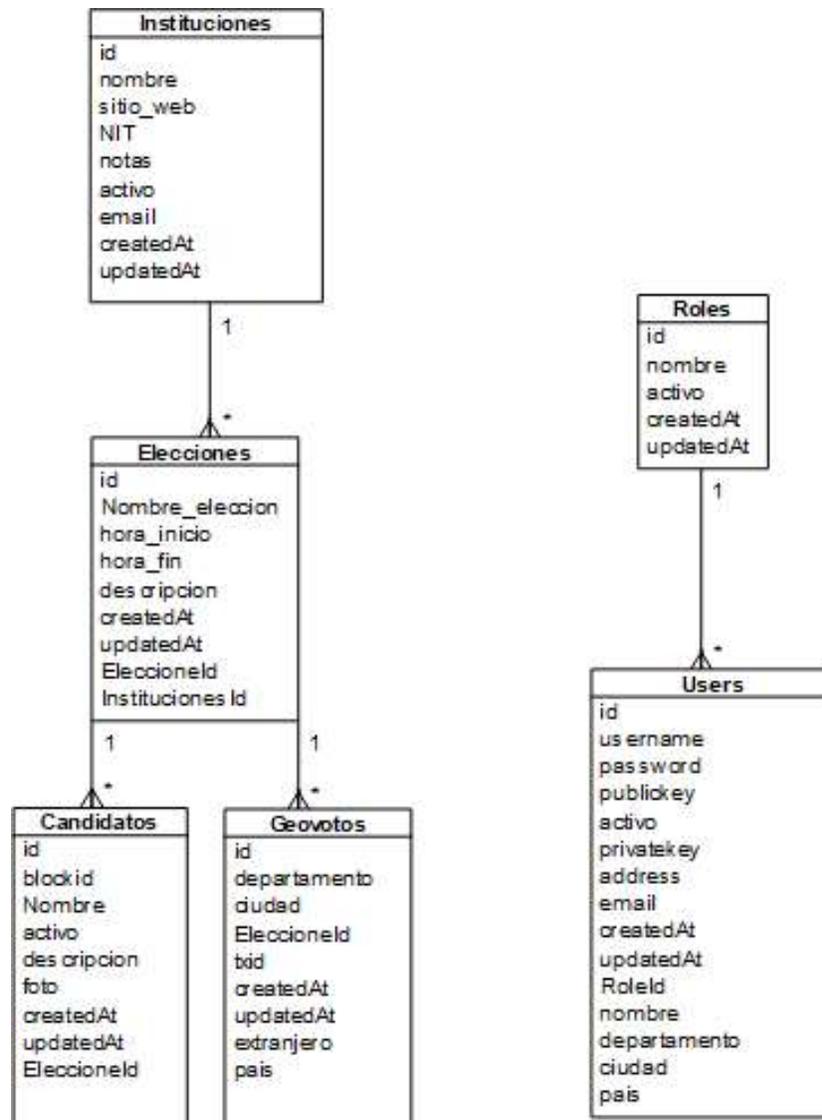


Figura 6.1. Diagrama Entidad-Relación.

6.2. Vista de procesos

6.2.1. Diagrama de actividad: creación de elecciones y candidatos

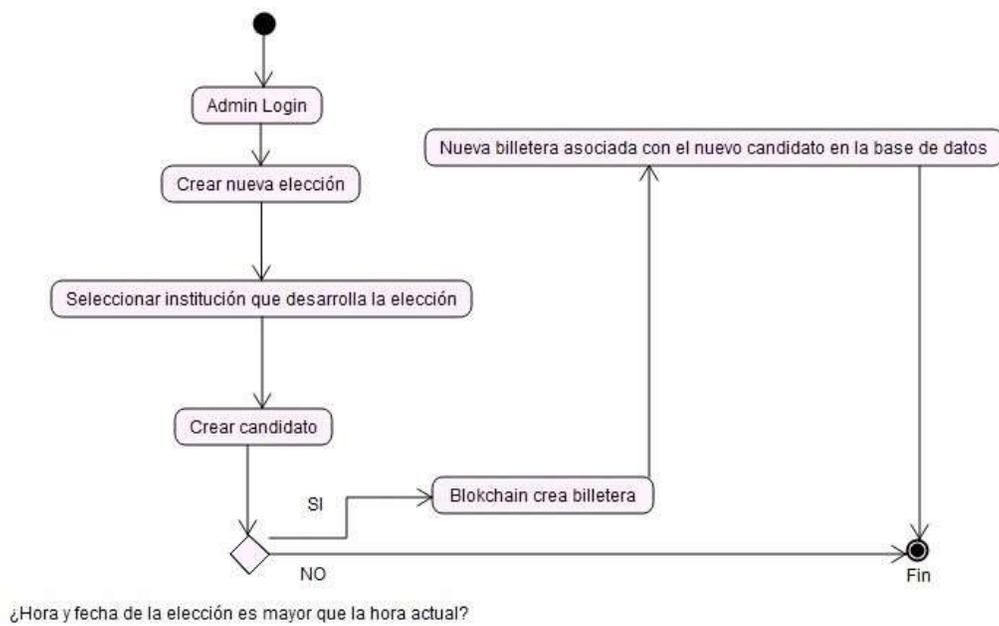


Figura 6.2. Diagrama de actividad: creación de elecciones y candidatos.

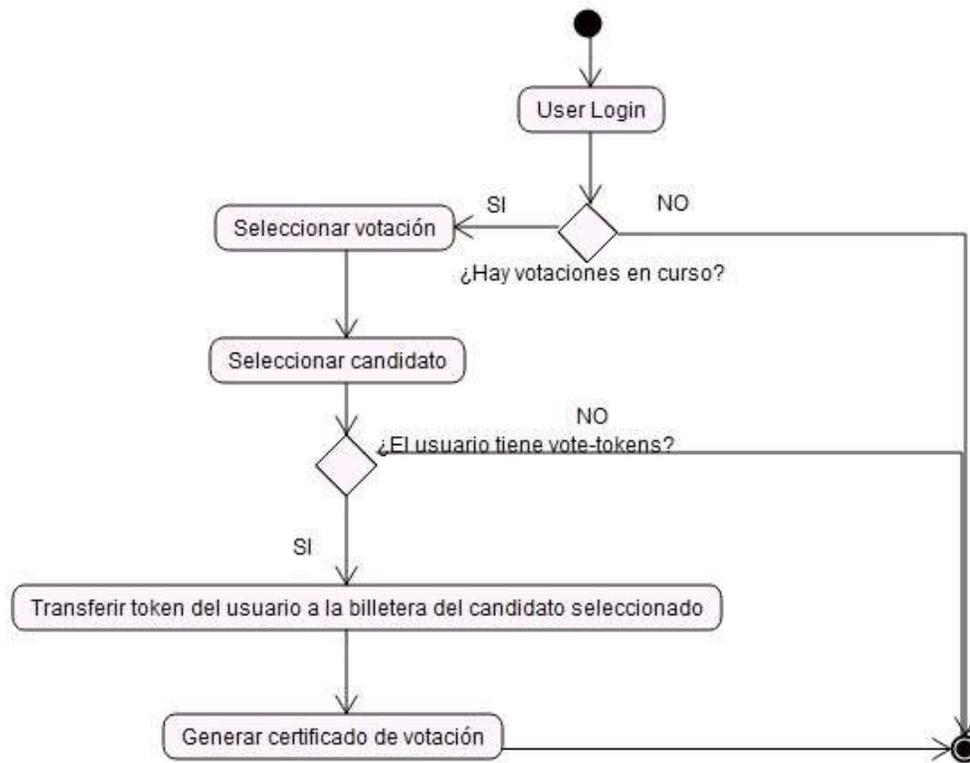
6.2.2. Diagrama de actividad: votación

Figura 6.3. Diagrama de actividad: votación.

6.2.3. Diagrama de actividad: ver resultados

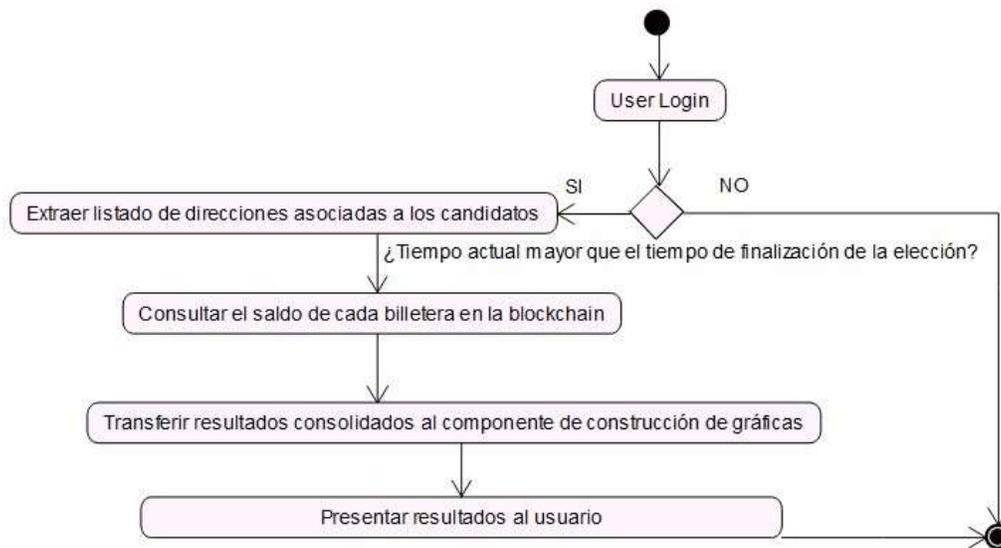


Figura 6.4. Diagrama de actividad: ver resultados.

6.3. Vista Lógica

6.3.1. Diagrama de secuencia: crear elecciones

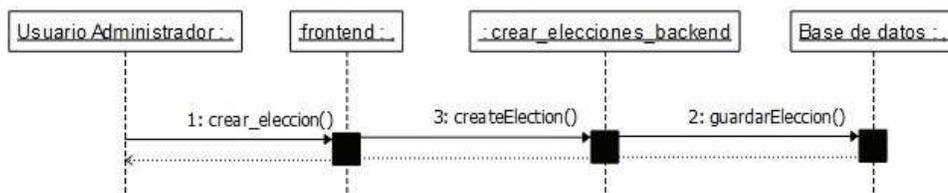


Figura 6.5. Diagrama de secuencia: crear elecciones.

6.3.2. Diagrama de secuencia: crear candidatos

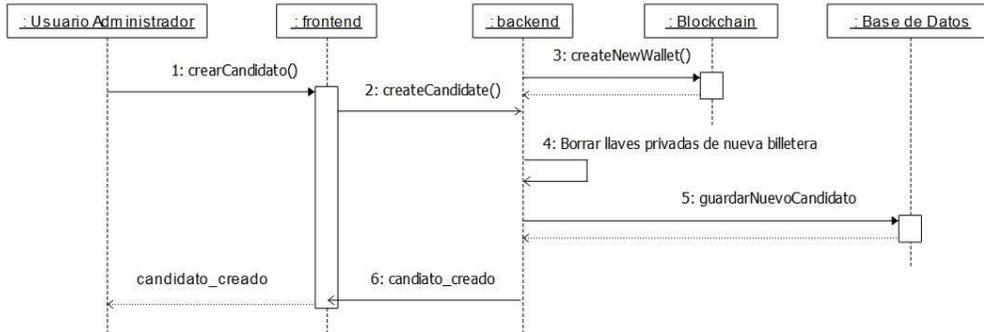


Figura 6.6. Diagrama de secuencia: crear candidatos.

6.3.3. Diagrama de secuencia: crear elecciones

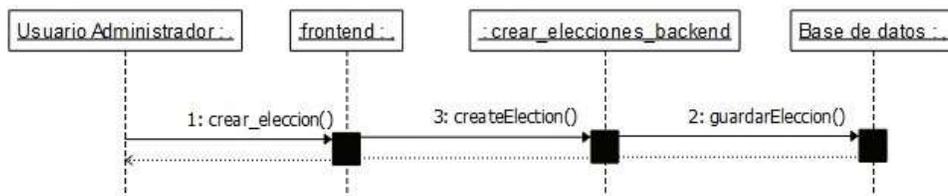


Figura 6.7. Diagrama de secuencia: crear elecciones.

6.3.4. Diagrama de secuencia: obtener resultados

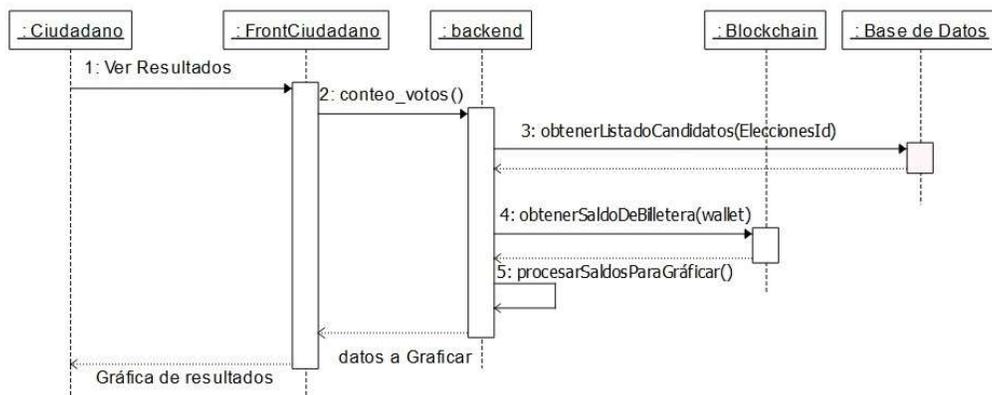


Figura 6.8. Diagrama de secuencia: obtener resultados.

6.4. Vista física

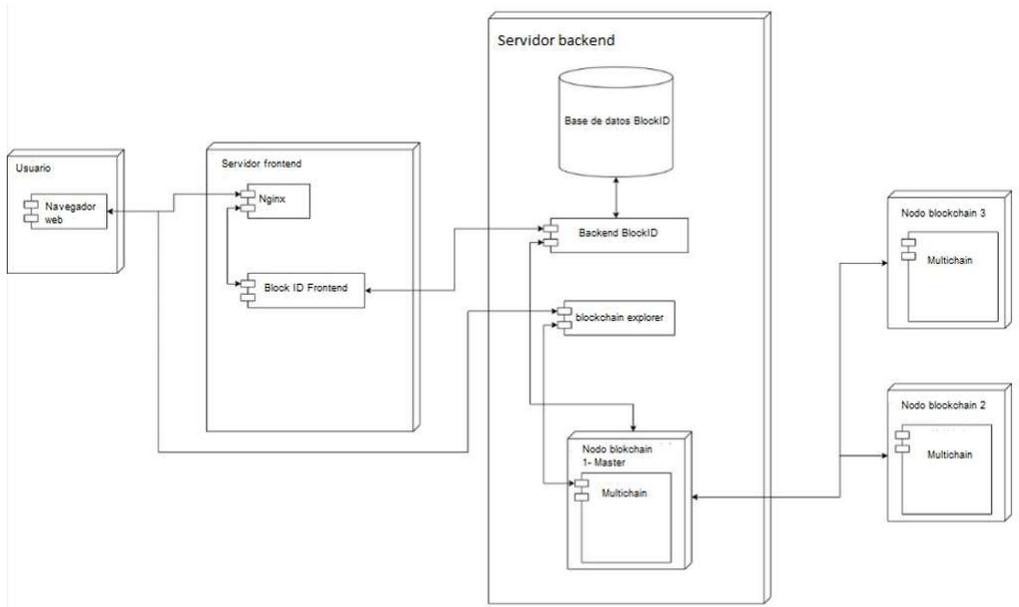


Figura 6.9. Vista física.

6.5. Escenarios o casos de uso

6.5.1. Caso de uso general

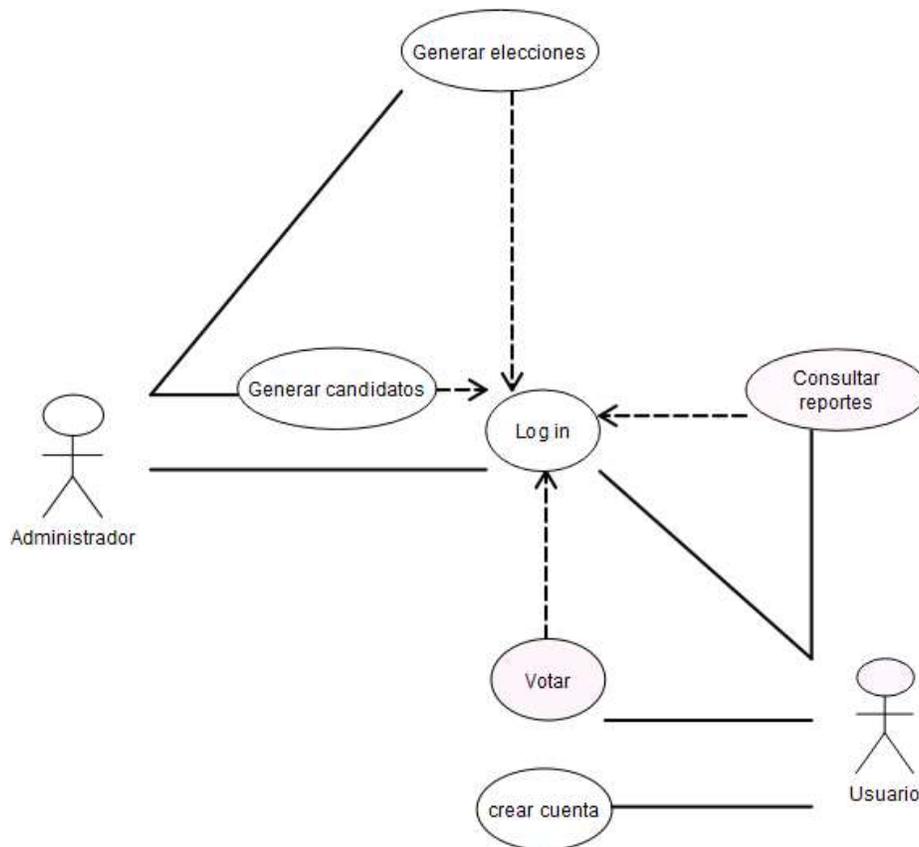


Figura 6.10. Caso de uso general.

6.5.2. Caso de uso: generación de candidatos

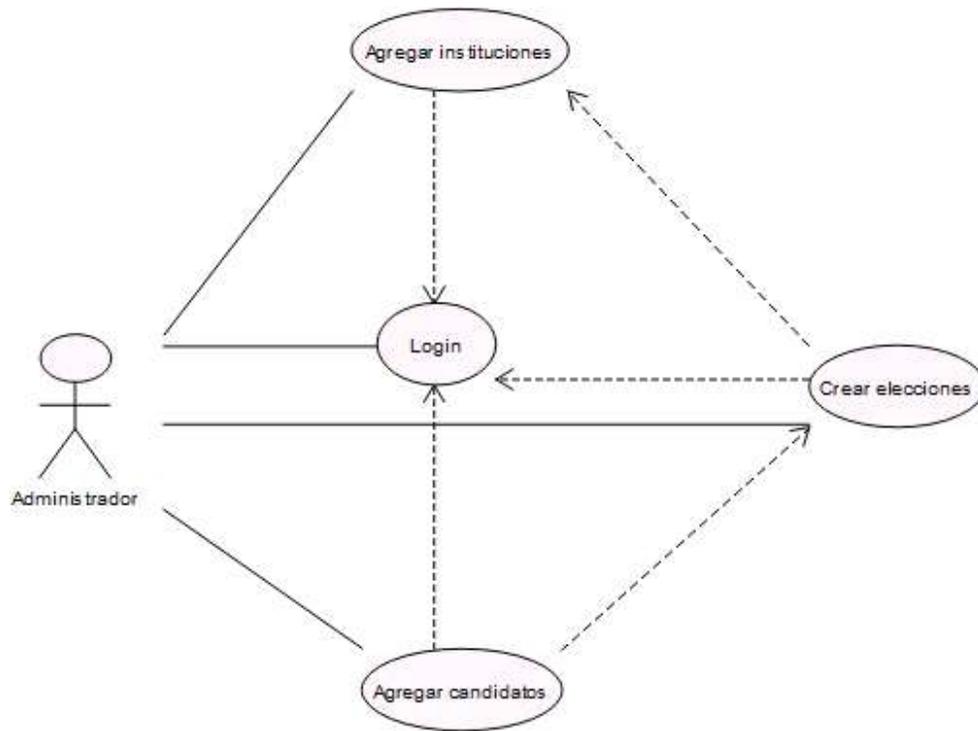


Figura 6.11. Caso de uso: generación de candidatos.

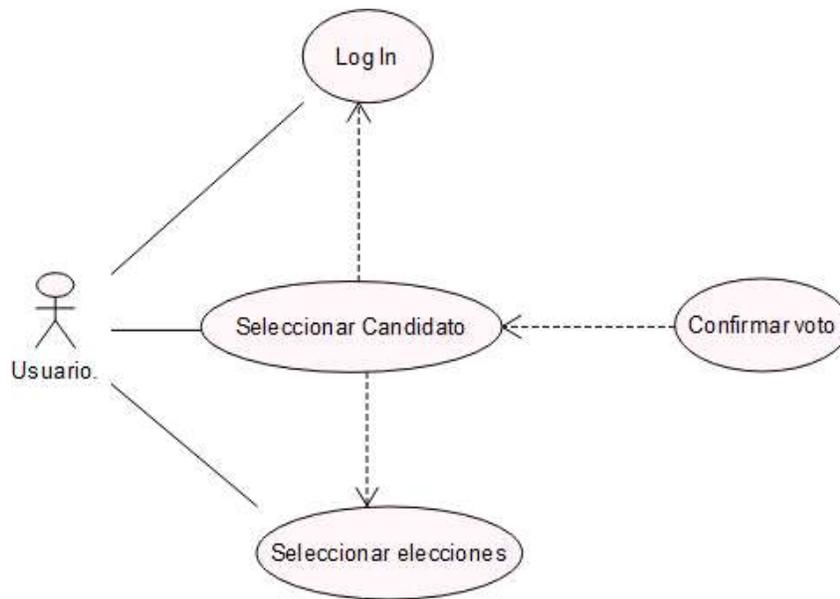
6.5.3. Caso de uso: votación

Figura 6.12. Caso de uso: votación.

Capítulo 7

Pruebas de rendimiento software

7.1. Pruebas de rendimiento de la aplicación

Las pruebas de rendimiento se realizaron usando los tres *endpoints* más representativos de la operación. Siendo estos: el *login*, el *endpoint* encargado de validar usuario en la plataforma web; consulta de resultados, el endpoint encargado de consultar los resultados de una elección; y el *endpoint* de votación, que realiza la transacción sobre la *blockchain* para generar el voto por un candidato agregado para las pruebas.

7.1.1. Prueba de Carga (*load testing*)

La prueba de carga permite identificar la cantidad de peticiones que pueden ser soportadas por un sistema. De esta forma, se podrá conocer el comportamiento de la aplicación cuando se aplican diferentes cargas (peticiones por minuto). Este tipo de prueba permitirá identificar errores cometidos en el proceso de desarrollo, que son responsables de una falla en particular o de bajo rendimiento. Para esta prueba se utilizaron 10 usuarios concurrentes, en donde se presentaron tiempos promedio de respuesta a las votaciones de 560 milisegundos, con una duración mínima de 86 milisegundos y máxima de 1.812 milisegundos. Es de acotar que los usuarios empleados en la prueba fueron concurrentes (los 10 usuarios votaron al mismo tiempo). Lo cual sucederá en periodos de cargas relativamente altas.

En la gráfica se puede notar cómo el *endpoint* con mayor tiempo de respuesta es el de *login*, esto es lo esperado en condiciones normales, ya que

es el *endpoint* encargado de generar el JWT (*Java Web Token*), el cual es empleado para autenticar todas las peticiones al *backend*.

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Votar	800	560	86	1812	578.95	0.000 %	2.29303	0.78	1.25	350.0
Login	800	1594	446	2612	299.68	0.000 %	2.29291	1.49	1.50	667.0
Obtener resultados	800	509	110	1855	488.49	0.000 %	2.29631	3.80	1.05	1694.0
TOTAL	2400	888	86	2612	686.15	0.000 %	6.85147	6.05	3.77	903.7

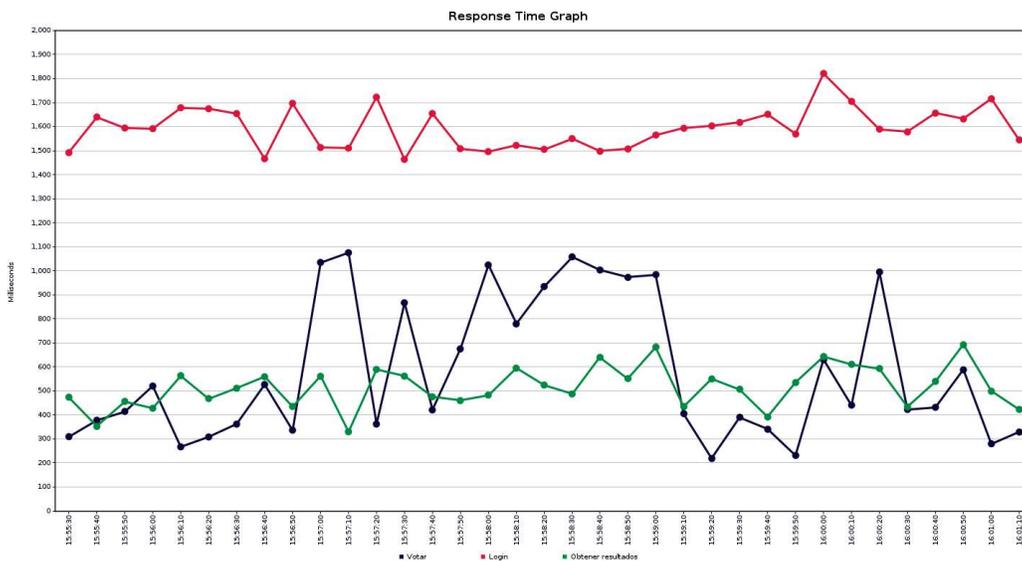


Figura 7.1. Tiempo de respuesta, prueba de carga.

7.1.2. Prueba de Estrés (*stress*)

La prueba de estrés permite conocer los límites que un sistema puede tolerar. En este tipo de pruebas el software es inundado con más peticiones de las que puede soportar, para comprender el comportamiento de la aplicación ante este posible escenario que enfrentan las aplicaciones web, como la desarrollada en esta tesis. Para esta prueba se utilizaron 100 usuarios concurrentes. Cabe resaltar que, a pesar de estar soportando más carga de la que el servidor actual puede manejar, el *endpoint* para consultar el resultado de las elecciones fue el único con una tasa de error del 0 %, si bien llegó a tener tiempos de respuesta de hasta un minuto y medio (129.204 milisegundos), el 100 % de las peticiones enviadas fueron resueltas satisfactoriamente. En contraste, el *endpoint* de votaciones fue el más afectado en medio de la prueba de estrés, con un 13.8 % de peticiones erróneas. De hecho, casi al final de la prueba, se ve un descenso considerable en los tiempos de respuesta del

endpoint de *login* y el de votaciones, fue durante este tiempo que el sistema rechazó las peticiones sin siquiera intentar procesarlas, por encontrarse bloqueado en medio de la inundación de peticiones.

Label	#Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Votar	2016	14752	89	57628	9987.55	13.790 %	2.68195	1.04	1.43	398.0
Login	1980	11164	278	129204	7598.66	3.283 %	2.67746	1.94	1.69	741.3
Obtener resultados	1916	11304	124	33531	7197.64	0.000 %	2.60226	4.30	1.18	1694.0
TOTAL	5912	12433	89	129204	8539.82	5.802 %	7.86493	7.17	4.25	933.0

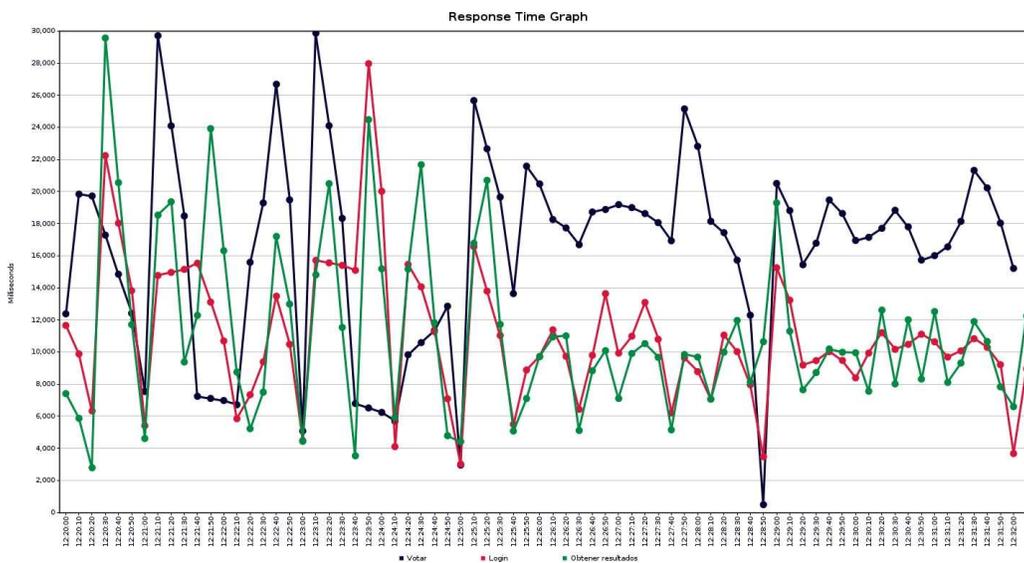


Figura 7.2. Tiempo de respuesta, prueba de estrés.

7.1.3. Prueba de Resistencia (*endurance*)

La prueba de resistencia consiste en enviar peticiones en diferentes intervalos de tiempo y en diferentes volúmenes, simulando horas pico y horas valle en el sistema. El objetivo es conocer el comportamiento de la aplicación luego de una carga extrema. En este caso en particular, se enviaron peticiones con 500 usuarios concurrentes, durante periodos aleatorios entre 1 y 15 minutos. Luego de la alta carga y congestión, la herramienta de pruebas disminuye los usuarios a 5 concurrentes, momento en el cual el sistema comienza a responder con normalidad, a pesar de haber soportado una congestión extrema. Se puede concluir con esta prueba, que el sistema puede recobrar su funcionamiento normal luego de periodos de carga extrema.

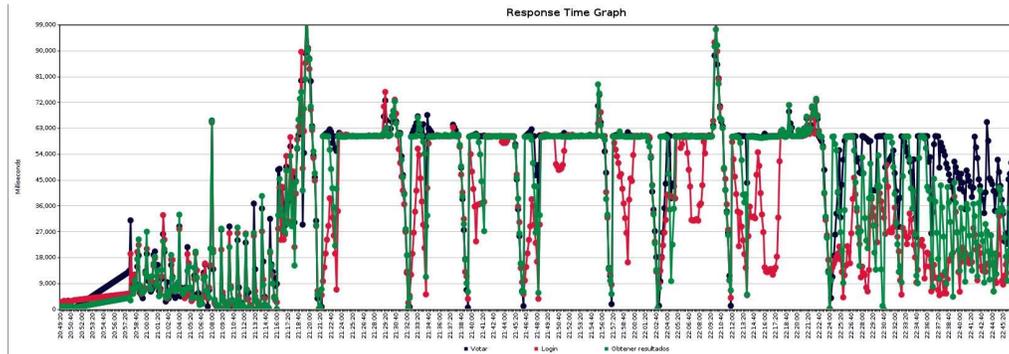


Figura 7.3. Tiempo de respuesta, prueba de resistencia.

7.1.4. Prueba de Escalabilidad (*scalability*)

Se configuró un clúster de escalabilidad horizontal en un proveedor de nube (Linode) que monitorea la carga del sistema y ante una carga excesiva configura nuevos servidores para responder a la misma. En esta prueba, se enviaron 30 usuarios concurrentes y al cabo de un minuto, se sube la carga a 500 usuarios concurrentes. Se puede evidenciar el atasco en las peticiones durante dos minutos, durante este tiempo el proveedor de nube detectó la congestión y encendió nuevas máquinas, reduciendo drásticamente el tiempo de respuesta, como se puede observar en la figura.

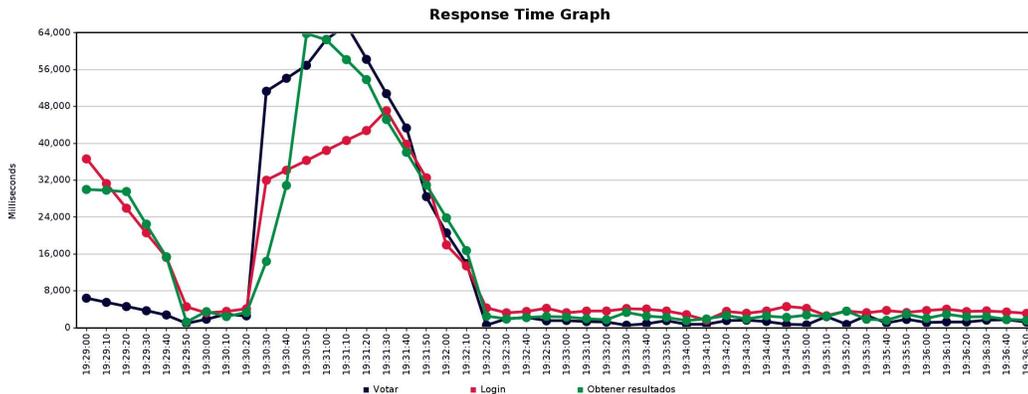


Figura 7.4. Tiempo de respuesta, prueba de escalabilidad.

Capítulo 8

Implementación y conclusiones

8.1. Caso de uso

Se realizaron varios sondeos electorales para intención de voto de las elecciones presidenciales del año 2022, las encuestas se han diseñado con base en los sondeos electorales que han venido haciendo varios medios de comunicación de Colombia. Para el caso de uso de este proyecto se han utilizado los siguientes candidatos: Camilo Romero, Alejandro Gaviria, Alejandro Char, Ángela Robledo, Camilo Romero, Dilian Francisca Toro, Sergio Fajardo, Federico Gutiérrez, Francia Márquez, Jorge Enrique Robledo, Juan Manuel Galán, Marta Lucia Ramírez, Enrique Peñalosa, Gustavo Petro, Juan Carlos Pinzón, Tomas Uribe, Germán Vargas Lleras y, por último, el voto en blanco o ninguno. Se realizaron varias pruebas en varios escenarios que se presentaron durante el desarrollo de este proyecto, entre ellas reuniones en conjunto con el CIDT de la UTP, Pereira 4.0, entre otras. La difusión de estas se realizó por medio de las redes sociales, periódicos locales como el Q'hubo y La Paz periodismo libre, además de la difusión en varias charlas de tecnología 4.0 de la ciudad de Pereira y eventos realizados con el CIDT de la UTP. Se realizaron un total de seis sondeos electorales, teniendo como el más importante y con más asistencia el realizado del día 15 de junio al 31 de junio, en donde se obtuvieron 138 votos.

8.2. Proceso de elecciones usuario

En esta sección se muestra cómo es el proceso de elecciones por parte de los usuarios, desde el momento que deciden participar en las elecciones hasta

el momento en el que depositan su voto y reciben el certificado electoral correspondiente.

8.2.1. Creación de cuenta

Los usuarios interesados en participar debían ir al sistema desplegado de BlokID que se aloja en la siguiente dirección web (<https://blockid.pulsatrix.co/>), como se muestra en la siguiente figura:

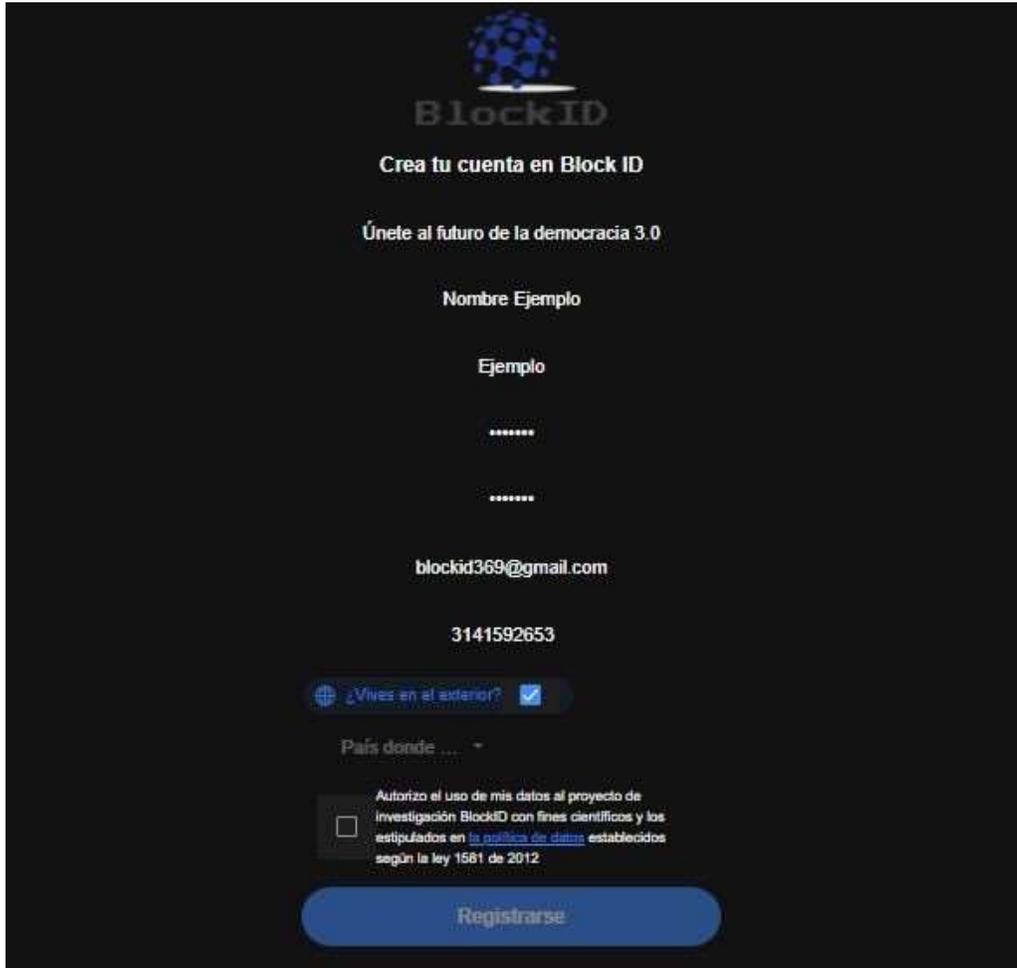


Figura 8.1. Landing page <https://blockid.pulsatrix.co/>.

Si el usuario ya estaba registrado en el sistema debía ingresar su usuario y contraseña, sino, debía realizar el proceso de registro que consta de la introducción de los datos personales del usuario como: nombre completo, nombre de usuario, contraseña, correo electrónico y celular; también datos de localización del usuario, como el departamento y la ciudad desde la cual está habilitado para votar, además se incluyó una opción para usuarios en el extranjero, como se muestra en las siguientes imágenes respectivamente:

The image shows a registration form for BlockID. At the top, there is a logo consisting of a blue globe with white dots, followed by the text "BlockID". Below the logo, the text reads "Crea tu cuenta en Block ID" and "Únete al futuro de la democracia 3.0". The form fields are as follows: "Nombre Ejemplo" with a placeholder "Ejemplo"; a password field with "*****"; a second password field with "*****"; an email field with "blockid369@gmail.com"; a phone number field with "3141592653"; a question "¿En que departamento y ciudad tienes inscrita la cédula para las próximas elecciones?" with two dropdown menus labeled "Departament..." and "Ciudad dond..."; a checkbox "¿Vives en el exterior?" with an unchecked box; and a consent section with a checkbox and the text "Autorizo el uso de mis datos al proyecto de investigación BlockID con fines científicos y los estipulados en la política de datos establecidos según la ley 1581 de 2012". At the bottom, there is a blue button labeled "Registrarse".

Figura 8.2. Registro de nuevos usuarios que se encuentran en el territorio nacional.



The image shows a registration form for BlockID. At the top, there is a logo consisting of a blue globe with the text "BlockID" below it. The main heading is "Crea tu cuenta en Block ID". Below this, it says "Únete al futuro de la democracia 3.0". The form fields are as follows: "Nombre Ejemplo" (Name), "Ejemplo" (Email), two masked password fields (each with six asterisks), the email address "blockid369@gmail.com", and the phone number "3141592653". There is a checkbox labeled "¿Vives en el exterior?" (Do you live abroad?) which is checked. Below this is a dropdown menu for "País donde ..." (Country where ...). At the bottom, there is a checkbox for data authorization with the text: "Autorizo el uso de mis datos al proyecto de investigación BlockID con fines científicos y los estipulados en la política de datos establecidos en la política de datos establecidos según la ley 1581 de 2012". A large blue button labeled "Registrarse" (Register) is at the bottom.

Figura 8.3. Registro de nuevos usuarios que se encuentran en el extranjero.

Por último, se pide a los usuarios autorizar el uso de los datos al proyecto de investigación BlockID con fines científicos y los estipulados en la política de datos establecidos por las propiedades fundamentales de la tecnología *blockchain* se conservarán 100 % privados. La política de manejo de datos empleada por BlockID con todos sus usuarios, se define de conformidad con la entrada en vigencia de la Ley Estatutaria 1581 de 2012, la cual tiene por objeto “dictar las disposiciones generales para la protección de datos personales y desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, así como el derecho a la información”.

8.2.2. Creación de billetera

Una vez creada la cuenta, se pide al usuario generar una identidad virtual (billetera ó llave pública) dando click en el botón **Registrarme para votar**, como se muestra a continuación:

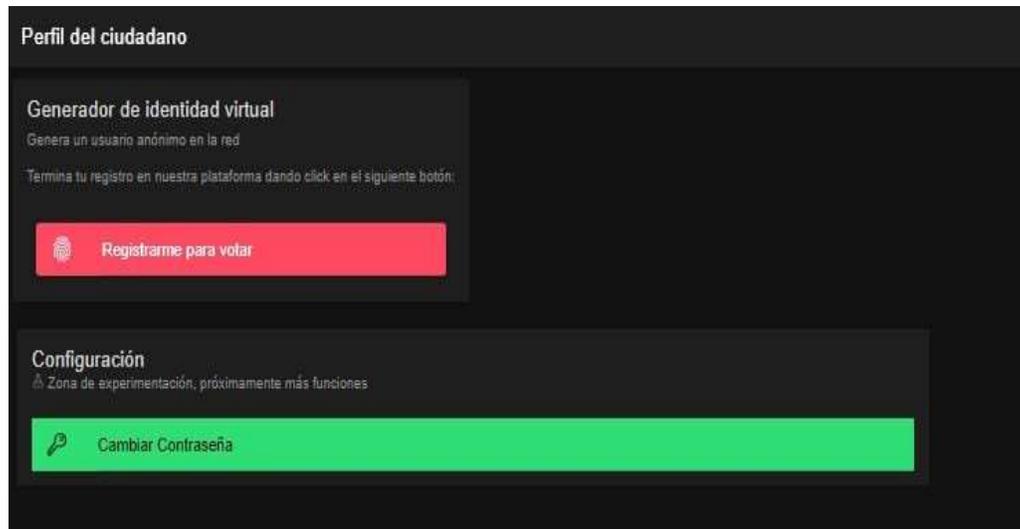


Figura 8.4. Generación de billetera electrónica paso 1.

Inmediatamente después de haber dado click en **Registrarme para votar**, un código que representa al usuario dentro de la red y un código QR salen en la pantalla, como se muestra en la figura:

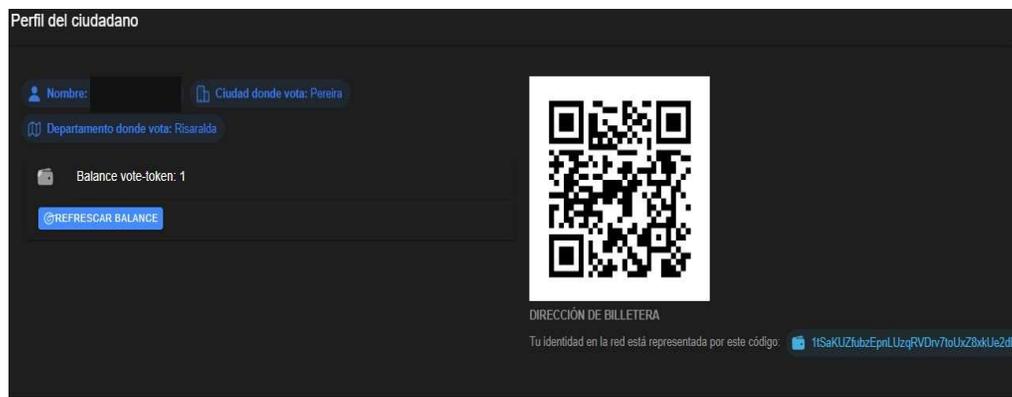


Figura 8.5. Generación de billetera electrónica paso 2.

Esta dirección de billetera es única por cada usuario y es el único dato visible representativo de cada usuario dentro del proceso y con el cual se puede auditar el correcto escrutinio de los votos.

8.2.3. Selección votación en curso y selección candidato

Una vez se haya creado la billetera y se tengan tokens suficientes para votar, el usuario puede seleccionar la votación disponible, seleccionar su candidato u opción predilecta, confirmar voto y por último generar el código único representativo del voto:

- Seleccionar la votación en curso en la cual se desee participar:

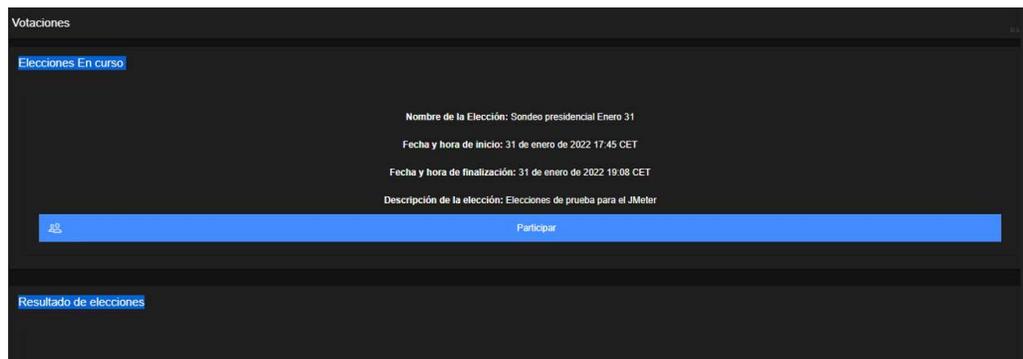


Figura 8.6. Selección de la elección de interés.

- Seleccionar candidato u opción:



Figura 8.7. Selección de una de las opciones presentes.

8.3. PROCESO DE ELECCIONES PARA EL ADMINISTRADOS DE LAS ELECCIONES85

- Confirmar voto:



Figura 8.8. Confirmación del voto emitido.

- Generar certificado electoral:



Figura 8.9. Certificación única del voto emitido.

8.3. Proceso de elecciones para el administrador de las elecciones

En esta sección se explica el procedimiento de creación de una elección, que consiste en 3 pasos principales:

- **Creación de la entidad encargada de las elecciones:** en este paso se pide al usuario administrados definir el nombre de la entidad que va a realizar las elecciones, el NIT, sitio web, email y notas adicionales en caso de haberlas, como se muestra en la siguiente imagen:

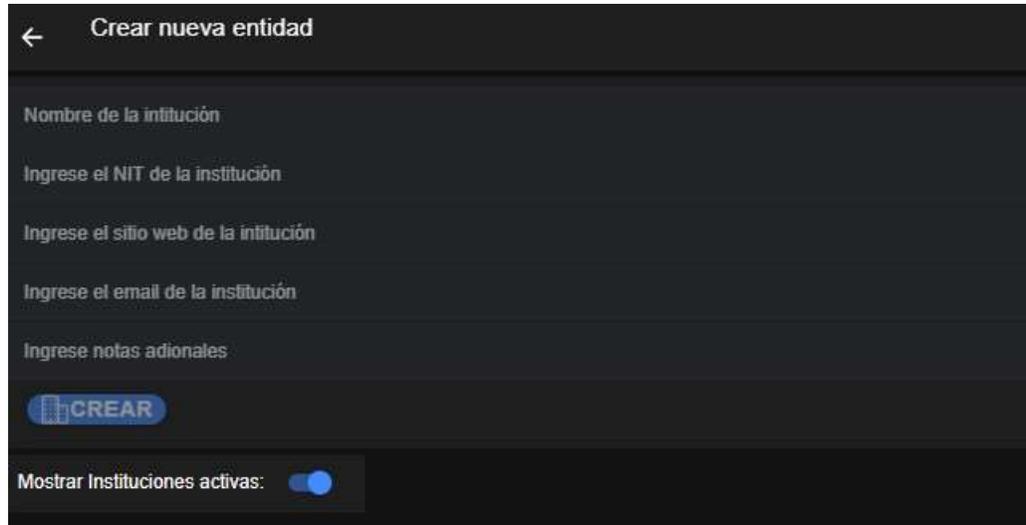
La imagen muestra una pantalla de un sistema de gestión de elecciones con el título "Crear nueva entidad". La interfaz es de color oscuro y contiene los siguientes elementos: un botón de retroceso en la esquina superior izquierda; un campo de texto para "Nombre de la institución"; un campo de texto para "Ingrese el NIT de la institución"; un campo de texto para "Ingrese el sitio web de la institución"; un campo de texto para "Ingrese el email de la institución"; un campo de texto para "Ingrese notas adicionales"; un botón azul con el texto "CREAR" y un icono de documento; y un interruptor de configuración etiquetado como "Mostrar Instituciones activas:" que está activado.

Figura 8.10. Creación de la institución que va a realizar las elecciones.

- **Creación de la elección:** en este paso, el usuario administrador genera las elecciones, las cuales deben ser referidas a una institución (paso anterior), debe ingresar el nombre, hora y fecha de inicio, hora y fecha de finalización y también se pide al administrador ingresar una descripción de las elecciones, como se muestra en la siguiente imagen:

8.3. PROCESO DE ELECCIONES PARA EL ADMINISTRADOS DE LAS ELECCIONES87



Figura8.11. Creación de las elecciones.

Hasta el momento no se han introducido los candidatos, ya que los candidatos se pueden agregar solo después de este paso, por eso se recomienda a los usuarios generar las elecciones con un tiempo de holgura para poder introducir los candidatos necesarios con los respectivos datos solicitados.

- **Creación de candidatos:** el último paso para la creación de unas elecciones en la plataforma de BlockID consiste en generar los candidatos que van a ser votados en las elecciones correspondientes, para poder realizar este paso se tienen que haber realizado de manera correcta los dos pasos anteriores, ya que los candidatos tienen que estar relacionados con la votación previamente creada, que a su vez esta relacionada con la institución administradora de las elecciones. La información requerida en este punto del proceso es: nombre del candidato, descripción del candidato y una imagen, la cual tiene que ser de dimensiones iguales para todos los candidatos u opciones introducidas.

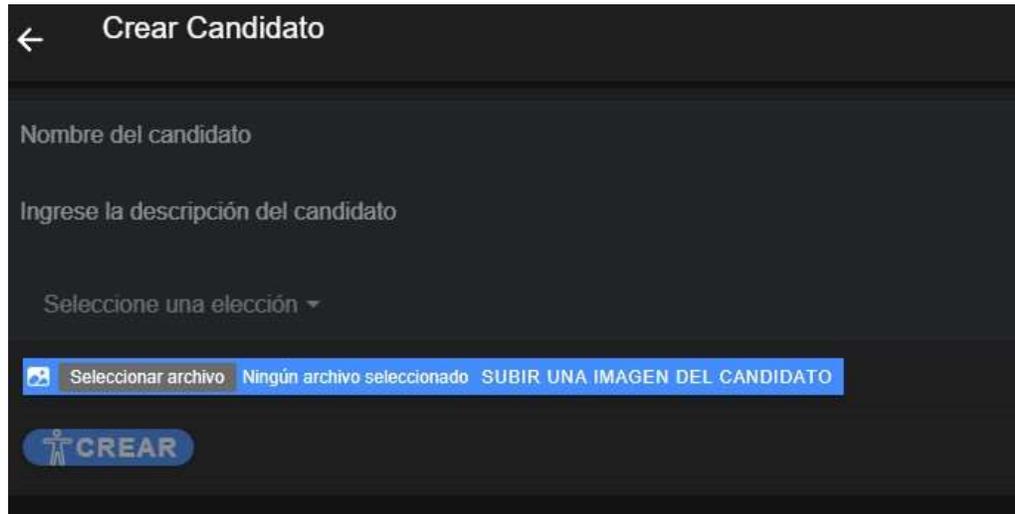


Figura 8.12. Creación de las elecciones.

8.4. Conclusiones

El proceso electoral en Colombia y en el mundo en general está sufriendo de una pérdida de confianza por parte de los ciudadanos, que se traduce en altas tasas de abstencionismo en las diferentes elecciones ordinarias de cada país, debido en gran parte a la corrupción que existe dentro del proceso democrático. Sin embargo, en los últimos años se ha venido viendo un brote de rabia e inconformidad por parte de los ciudadanos, reflejada en múltiples marchas y protestas exigiendo un mejor manejo de los recursos y procesos administrativos del estado, es allí donde la tecnología *blockchain* y sus propiedades tienen el potencial de reemplazar y mejorar muchos procesos públicos del estado en pro de la sociedad. Pero para ello se necesita educar a la sociedad, primero en la concientización sobre la existencia de esta tecnología, segundo para que conozcan cómo funciona y tercero concientizar a los ciudadanos sobre los beneficios que traería esta tecnología aplicada no solo en la modernización del sistema electoral, sino también en otras áreas del estado.

Este proyecto puede llegar a ser implementado en instituciones educativas para sus elecciones de representantes estudiantiles, con el objetivo de generar un proceso electoral más seguro y transparente, al tiempo que permite difundir la tecnología ante un gran número de personas, ampliando así la

del potencial que tiene la tecnología *blockchain*.

El desarrollo de un sistema de votaciones basado en *blockchain* es relativamente económico en comparación con los altos costos de logística y material impreso que se consume en los procesos electorales actuales. Por lo cual es válido argumentar que además de evitar el fraude electoral, este tipo de sistemas genera un impacto ambiental positivo.

El desarrollo del presente prototipo de un sistema de votación electrónica basada en *blockchain*, es un primer paso para abrir el debate en la población colombiana sobre la importancia de la modernización del estado, específicamente del uso de la *blockchain* para agilizar y dar mayor transparencia a los procesos estatales.

Referencias

- [1] S. A. Abeyratne y R. P. Monfared, “Blockchain ready manufacturing supply chain using distributed ledger”, *International Journal of Research in Engineering and Technology* 5.9 (2016), págs. 1-10.
- [2] R. Adeodato y S. Pournouri, “Secure implementation of E-governance: A case study about Estonia”, *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*. Springer, Cham, 2020, págs. 397-429.
- [3] T. Ahram y col., “Blockchain technology innovations”, *2017 IEEE Technology Engineering Management Conference (TEMSCON)*. 2017, págs. 137-141. DOI: 10.1109/TEMSCON.2017.7998367.
- [4] D. Allen y col., “The Economics of Crypto-Democracy”, *SSRN Electronic Journal* (ene. de 2017), págs. 63-73. ISSN: 1573-7128. DOI: 10.2139/ssrn.2973050.
- [5] J. Alves y A. Pinto, “On the use of the blockchain technology in electronic voting systems”, *International Symposium on Ambient Intelligence*. Springer. 2018, págs. 323-330.
- [6] M. Atzori, “Blockchain technology and decentralized governance: Is the state still necessary?”, *Available at SSRN 2709713* (2015).
- [7] T. Baltic, *Estonian Electronic ID-Card Application Specification Prerequisites to the Smart Card Differentiation to previous Version of EstEID Card Application*.
- [8] I. Bashir, *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*. Packt Publishing Ltd, 2018.

- [9] D. Bayer, S. Haber y W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping", *Sequences II*. Springer, 1993, págs. 329-334.
- [10] B. Bogucki, "Buying Votes in the 21st Century: The Potential Use of Bitcoins and Blockchain Technology in Electronic Voting Reform", *Asper Rev. Int'l Bus. & Trade L.* 17 (2017), pág. 59.
- [11] N. S. Burhanuddin y col., "Blockchain in Voting System Application", *International Journal of Engineering Technology* 7.4.11 (2018), págs. 156-162. ISSN: 2227-524X. DOI: 10.14419/ijet.v7i4.11.20793. URL: <https://www.sciencepubco.com/index.php/ijet/article/view/20793>.
- [12] K. Christidis y M. Devetsikiotis, "Blockchains and smart contracts for the internet of things", *Ieee Access* 4 (2016), págs. 2292-2303.
- [13] R. Cooley, S. Wolf y M. Borowczak, "Blockchain-based election infrastructures", *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE. 2018, págs. 1-4.
- [14] E. M. Dogo y col., "Blockchain 3.0: Towards a secure ballotcoin democracy through a digitized public ledger in developing countries", *I-manager's Journal on Digital Signal Processing* 6.2 (2018), págs. 24-35.
- [15] J. Barrati-Esteve, B. Goldsmith y J. Turner, "International experience with e-voting", *Norwegian E-Vote Project. International Foundation for Electoral Systems. Document disponible online la dirección <http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/%7E/media/B7FB434187E943C18F4D4992A4EF75DA.pdf>* (2012).
- [16] J. Frizzo-Barker y col., "Blockchain as a disruptive technology for business: A systematic review", *International Journal of Information Management* 51 (2020), pág. 102029.
- [17] J. W. Getzels, "Reviews: DAVID L. SILLS (Ed.) International Encyclopedia of the Social Sciences. 17 Volumes. New York: Macmillan Free Press, 1968. 9750+ xxx pp. 495.00", *American Educational Research Journal* 6.4 (1969), págs. 677-685.
- [18] M. Golder, "Democratic electoral systems around the world, 1946-2000", *Electoral Studies* 24.1 (2005), págs. 103-121.
- [19] S. Haber y W. S. Stornetta, "How to time-stamp a digital document", *Conference on the Theory and Application of Cryptography*. Springer. 1990, págs. 437-455.

- [20] S. Heiberg, P. Laud y J. Willemsen, “The application of i- voting for Estonian parliamentary elections of 2011”, *International Conference on E-Voting and Identity*. Springer, págs. 208-223.
- [21] L. Helfrich, “Abstención y participación electoral en Colombia y América Latina”, *Análisis Político* 23 (1994), págs. 98-104.
- [22] F. Hjálmarsson y col., “Blockchain-based e-voting system”, *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE. 2018, págs. 983-986.
- [23] M. San-Jun, “Blockchain government-a next form of infrastructure for the twenty-first century”, *Journal of Open Innovation: Technology, Market, and Complexity* 4.1 (2018), pág. 7.
- [24] K. Mehboob-Khan, J. Arshad y M. Mubashir-Khan, “Secure digital voting system based on blockchain technology”, *International Journal of Electronic Government Research (IJEGR)* 14.1 (2018), págs. 53-62.
- [25] P. B. Kruchten, “The 4+1 view model of architecture”, *IEEE software* 12.6 (1995), págs. 42-50.
- [26] N. Kshetri y J. Voas, “Blockchain-enabled e-voting”, *Ieee Software* 35.4 (2018), págs. 95-99.
- [27] J. W. Lamare, “Eva Etzioni-Halevy. Political Manipulation and Administrative Power: A Comparative Study”, *The ANNALS of the American Academy of Political and Social Science* 453.1 (1981), págs. 256-257.
- [28] F. Lehoucq, “¿Qué es el fraude electoral? Su naturaleza, sus causas y consecuencias”, *Revista mexicana de sociología* 69.1 (2007), págs. 1-38.
- [29] D. F. Maesa y P. Mori, “Blockchain 3.0 applications survey”, *Journal of Parallel and Distributed Computing* 138 (2020), págs. 99-114.
- [30] S. Manski, “Building the blockchain world: Technological commonwealth or just more of the same?”, *Strategic Change* 26.5 (2017), págs. 511-522.
- [31] D. Mingxiao y col., “A review on consensus algorithm of blockchain”, *2017 IEEE international conference on systems, man, and cybernetics (SMC)*. IEEE. 2017, págs. 2567-2572.

- [32] T. Moura y A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence", *Proceedings of the 18th annual international conference on digital government research*. 2017, págs. 574-575.
- [33] R. R. Mukkamala y col., "Blockchain for social business: Principles and applications", *IEEE Engineering Management Review* 46.4 (2018), págs. 94-99.
- [34] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", *Decentralized Business Review* (2008), pág. 21260.
- [35] M. Nofer y col., "Blockchain", *Business & Information Systems Engineering* 59.3 (2017), págs. 183-187.
- [36] S. Osmanski, *What Are the Environmental Impacts of Different Voting Methods?* [En línea]. Disponible en <https://www.greenmatters.com/p/environmental-impacts-of-voting>. (accessed: 04.12.2020).
- [37] M. Pawlak, A. Poniszewska-Marañda y N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system", *Procedia Computer Science* 141 (2018), págs. 239-246.
- [38] R. Qi y col., "Blockchain-Powered Internet of Things, E-Governance and E-Democracy", *E-Democracy for smart cities* (2017), págs. 509-520. DOI: https://doi.org/10.1007/978-981-10-4035-1_17.
- [39] P. Racsco, "Blockchain and Democracy", *Society and Economy* 41.3 (2019), págs. 353-369.
- [40] M. Skolnik, "The Effects of Corruption on Various Forms of Political Participation in Colombia", *Latin American Policy* 11.1 (2020), págs. 88-102.
- [41] D. Springall y col., "Security analysis of the Estonian internet voting system", *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 2014, págs. 703-715.
- [42] W. Viriyasitavat y Z. Bi., (2019), "Blockchain characteristics and consensus in modern business processes", *Journal of Industrial Information Integration*, Vol. 13, pp. 32-39, available at: <https://doi.org/10.1016/j.jii.2018.07.004>
- [43] Z. Zheng y col., "Blockchain challenges and opportunities: A survey", *International Journal of Web and Grid Services* 14.4 (2018), págs. 352-375.