Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Tema:

Propuesta de una metodología de votaciones electrónicas utilizando la plataforma de *blockchain* y la firma digital en Costa Rica

Estudiante:

Blanco Fiatt, Miguel Ángel

Setiembre 2018

TABLA DE CONTENIDO

LISTA DE FIGURAS

Capítulo 1. Introducción

1.1 Generalidades

Costa Rica es un país democrático desde su independencia de España en 1821. La palabra democracia proviene del griego *demos* (pueblo) y *kratos* (poder), esto quiere decir que es el gobierno del pueblo, por el pueblo y para el pueblo, lo que implica que cada ciudadano participa de forma libre en la elección de los gobernantes. La forma en la que funciona en Costa Rica es por medio del voto directo, el cual tiene otorgadas por la Constitución Política de 1949 cuatro características: universal, libre, directo y secreto.

En Costa Rica, el Tribunal Supremo de Elecciones en su función de administración del proceso de elecciones, es el responsable de la organización, dirección y control de todos los actos relativos al sufragio.

Las votaciones son de forma presencial y para votar la persona debe estar debidamente empadronada en la respectiva junta receptora de votos, debe presentar su cédula vigente al día de las elecciones y en el caso de que tenga que renovarla o sacar una nueva este proceso se debe realizar antes del cierre del padrón electoral.

En la presente investigación se presenta, con base en la firma digital y la plataforma *blockchain*[1], una propuesta para un sistema de votaciones electrónicas.

[1]*Blockchain* (cadena de bloques, en inglés) comprende una base de datos distribuida en la que cada ítem de la base de datos dispone de un sello de tiempo y de un enlace a un documento anterior, de forma que una vez sellado dicho ítem, es imposible -teóricamente- modificarlo (Blockchain, n. d.).

1.2 Antecedentes del problema

Actualmente, el sistema de votaciones en Costa Rica se realiza de forma física en lugares específicos de votaciones y hace que la logística de desplazamiento de los votantes pueda complicarse por diferentes motivos, por ejemplo: una persona que se cambió de domicilio de San José a Guanacaste y no actualizó su situación en el Tribunal Supremo de Elecciones; otro ejemplo lo constituyen personas que se encuentran fuera del país, personas con discapacidades o las que se encuentran hospitalizadas. Otro aspecto que toma relevancia es lo delicado y lento del proceso de conteo manual de votos para verificar los resultados, tanto parciales como finales.

1.3 Definición y descripción del problema

La logística de permitir que todas las personas tengan la posibilidad de votar es muy compleja y esto hace que se eleve el costo de las elecciones a nivel nacional y, además, hay ciudadanos que quedan excluidos por diferentes motivos.

Como se mencionó, si una persona cambia su domicilio, pero no lo reporta, esta tendría que desplazarse desde su nuevo domicilio al lugar de votación asignado, las personas enfermas también quedan fuera de las votaciones porque no pueden abandonar el hospital y en cuanto a los residentes en el exterior, poner puntos de votación en todos los países es complicado. En la actualidad, Costa Rica tiene 52 consulados en 42 países y para el 31 de enero del 2016, 26.459 costarricenses estaban empadronados en los consulados de Costa Rica en el extranjero.

Además, bajaría el costo de las votaciones ya que en este momento el costo promedio por votante es de ₡1.459, pero garantizar que una persona indígena tenga acceso al voto significa una inversión de más del doble de esa cifra (₡3.748, descartando el efecto de la inflación, a partir de datos de las elecciones del 2016) y representa un gasto cuatro veces mayor para el caso de quienes votan en el extranjero (₡6.773, en términos reales a partir de datos del 2014) (Murillo, 2017).

En el caso del cantón de Talamanca, casi la mitad de los electores no fueron a ejercer el voto en el 2014, esto significó una pérdida de 12 millones de colones para el país. Al implantar una metodología de votaciones electrónicas se eliminarían estas pérdidas, ya que si una persona no va a votar no implicaría un gasto.

Asimismo, el conteo de los votos se haría en tiempo real ya que los votos se asignarían inmediatamente al candidato y se eliminaría la posibilidad del error humano en el conteo de las votaciones y no hay posibilidad de que se presente algún problema en el transporte de las papeletas en el momento de enviarlas a las urnas o cuando se devuelven de las urnas, por lo que tampoco habría papeletas sobrantes las cuales se podrían utilizar para realizar algún tipo de fraude electoral.

1.4 Justificación

Al utilizar la plataforma *blockchain* y la firma digital para las votaciones en el nivel nacional, se puede reducir el costo del proceso y, a la vez, se podría disminuir el porcentaje de abstencionismo al facilitar la emisión del voto.

Además, las votaciones electrónicas reducirían la deuda política al reducir los gastos en los que incurren los partidos políticos para el transporte de votantes. Por otro lado, agilizarían el cómputo de los resultados, el cual sería expedito y con una seguridad aún mayor que el proceso manual.

De esta forma, por medio de la solución propuesta en este documento, se permitiría que las personas que se encuentren en zonas alejadas, fuera del país o no puedan movilizarse a los centros de votación puedan ejercer su derecho al tener acceso a un dispositivo que tenga conexión a la plataforma.

Con esta propuesta también se lograrían ahorros significativos en el costo de impresión, custodia y traslado de papeletas, a la vez, mejoraría la seguridad al descentralizar las votaciones, con lo además se lograría la prevención de fraude electoral.

1.5 Viabilidad

1.5.1 Punto de vista técnico

Desde un punto de vista técnico el proyecto es viable pues solamente se requeriría que cada votante tenga un certificado de firma digital, acceso a un dispositivo con lector para el certificado digital y conexión a Internet. Esto se puede lograr si se dota a todos los centros educativos a nivel nacional con computadoras, según la cantidad de votantes que reciban, además, disponiendo de equipos similares en hospitales, cárceles, embajadas y consulados, para que asistan quienes no tengan computadora y acceso a Internet con las características requeridas.

1.5.2 Punto de vista operativo

Desde un punto de vista operativo el proyecto es viable ya que la plataforma de *blockchain* es robusta y se ha utilizado desde 2009 para el *Bitcoin*[2], al ser descentralizada da seguridad a las votaciones y por su implementación permite mantener el anonimato requerido por la ley para el sufragio.

1.5.3 Punto de vista económico

Desde un punto de vista económico la implementación de las votaciones utilizando una plataforma de *blockchain* sería viable ya que permite un ahorro en la logística de distribución y el costo de impresión de las papeletas y los gastos conexos en suministros, también reduciría el costo

[2] Bitcoin, moneda digital creada por un programador o grupo de programadores anónimo conocido como Satoshi Nakamoto en el 2009. (Gregersen)

por votante al minimizar la cantidad de personal necesario para las votaciones y sus gastos colaterales de transporte y alimentación, también la deuda política bajaría al eliminar el traslado de los votantes.

Además, esta propuesta no implica ningún tipo de equipo electrónico especial que requiera de inversión grande por parte del TSE, de hecho, debido a que la propuesta busca que los votantes utilicen su propio equipo para ejercer el voto reduce la cantidad de equipos que el TSE tendría que comprar para poner en los centros de votación para la gente que por diferentes motivos no pueda realizar la votación desde su propio dispositivo. A la vez, debido a que se utiliza la plataforma de *blockchain* tampoco requiere de servidores ya que el procesamiento y almacenamiento de la información estaría distribuido en los nodos que formen parte.

1.6 Objetivos

1.6.1 Objetivo general

Proponer una metodología para votaciones electrónicas utilizando la plataforma de *blockchain* y la firma digital en Costa Rica

1.6.2 Objetivos específicos

A. Describir los métodos de cifrado de firma digital.
B. Explicar la forma de trabajo de la plataforma de *blockchain* y cómo pueden prevenirse fraudes.
C. Escoger una plataforma de *blockchain* existente que sirva para las votaciones electrónicas nacionales.
D. Analizar la factibilidad técnica de implementación de un sistema de votaciones con las características propuestas.

E. Investigar la forma en la que puede mantenerse el anonimato del voto una vez utilizada la firma digital.

F. Verificar la validez jurídica del voto electrónico en el medio nacional.

1.7 Alcances y limitaciones

1.7.1 Alcances

- Se explica la plataforma de *blockchain* y cómo se puede utilizar como una plataforma para las votaciones electrónicas.
- Se analizan las ventajas y desventajas de la utilización de la plataforma *blockchain* para las votaciones.
- Se explica el uso y los beneficios de la firma digital y cómo esta se podría utilizar para el control de votantes.

1.7.2 Limitaciones

- Esta tesis se limita a la propuesta del método de votación y descripción de la plataforma, no se realiza ninguna aplicación o propuesta de la aplicación para realizar las votaciones.

Capítulo 2. Marco teórico

En esta tesis se analiza la propuesta de las votaciones electrónicas utilizando la plataforma de *blockchain* y la firma digital en Costa Rica, por lo que se debe comenzar por explicar los conceptos y las características de la firma digital, la plataforma de *blockchain* y el cifrado de datos para mantener el derecho al voto secreto y directo.

2.1 Votaciones en Costa Rica

2.1.1 Historia de las votaciones en Costa Rica

Cuando Costa Rica se unió a la República Federal Centroamericana en el año 1825, en este proceso se encontraban sectores que querían incorporarse a la Federación y los que no querían incorporarse, para la resolución de estos conflictos se optó por continuar con la normativa que estaba definida en la Constitución de Cádiz de 1812, por lo que se promovió la Ley Fundamental del Estado Libre de Costa Rica, basada en dicha constitución. En esta se estableció el sistema de sufragio indirecto en tres grados, los cuales eran las Juntas Populares, las de Parroquia y las de Partido, estas para la elección de los diputados del Poder Legislativo y los puestos de los Poderes Ejecutivo, Judicial y Conservador. Este sistema se dio de la siguiente forma: las Juntas Populares elegían a los electores de Parroquia quienes, a la vez, votaban por los electores de Partido. En esta constitución el sufragio era censitario, limitando así el derecho a votar únicamente a personas que poseían cierta cantidad de bienes o dinero, lo cual hacía que el poder se mantuviera en la clase alta de Costa Rica.

Estas características del voto sufrieron algunos cambios, pero siempre se mantenía el sufragio censitario, se implantó el voto directo y se eliminó varias veces a través de diversas

constituciones hasta la Constitución de 1949 y Constitución actual en la que se le concedió el derecho al voto a la mujer y en la que se logró consolidar el voto directo, que, además, le dio carácter de secreto y obligatorio.

2.1.2 Estado actual del voto en Costa Rica

Para que el voto cumpla la función cívica otorgada en la Constitución de 1949, es necesario que se cumplan ciertos requisitos, los cuales son el artículo 90: "La ciudadanía es el conjunto de derechos y deberes políticos que corresponde a los costarricenses mayores de dieciocho años" y el artículo 93 de la Constitución Política: "El sufragio es función cívica primordial y obligatoria y se ejerce ante las Juntas Electorales en votación directa y secreta, por los ciudadanos inscritos en el Registro Civil."

De estos artículos se puede concluir que el voto es un derecho universal, lo que quiere decir que deben practicarlo todos los ciudadanos sin distinción alguna y sin sujeciones a ningún tipo de condición, más que las impuestas previamente por la ley en lo que a limitación del ejercicio de la ciudadanía respecta. Además, el voto debe ser secreto, ya que es un acto personal que se emite de manera directa y secreta, para que el elector no sufra ningún tipo de persecución política. El voto también tiene que ser directo, esto quiere decir que los votantes son los que se presentan ante las juntas electorales a votar directamente por los candidatos sin la necesidad de elegir un tercero para que este ejerza el voto. Por último, el voto debe ser libre, lo que significa que el votante no debe ser coaccionado o intimidado por nadie para que ejerza su derecho de votar.

Según el Diccionario CAPEL "las elecciones no pueden ser libres si quienes gobiernan pueden manejarlas para afianzarse en poder, porque las elecciones libres tienen como finalidad esencial la legitimación y la limitación del poder".

2.2 Criptografía

Se comienza por definir el término *criptografía*, el cual proviene del griego *kriptos* (oculto) y *grafos* (escritura). El diccionario de la RAE (2001) lo define como *"*el arte de escribir con clave secreta o de un modo enigmático".

La Criptografía es la ciencia que se encarga de estudiar las técnicas empleadas para cifrar la información y así hacerla inaccesible a todas aquellas personas que tengan acceso a esta, pero no tengan el permiso para accederla. Mediante la Criptografía es posible garantizar la confidencialidad, la integridad y la autenticidad de los mensajes (Vieites, Enciclopedia de la Seguridad Informática, 2011).

Los sistemas criptográficos se clasifican en dos grandes grupos, los cuales son los simétricos y los asimétricos, esto según el tipo de clave utilizada.

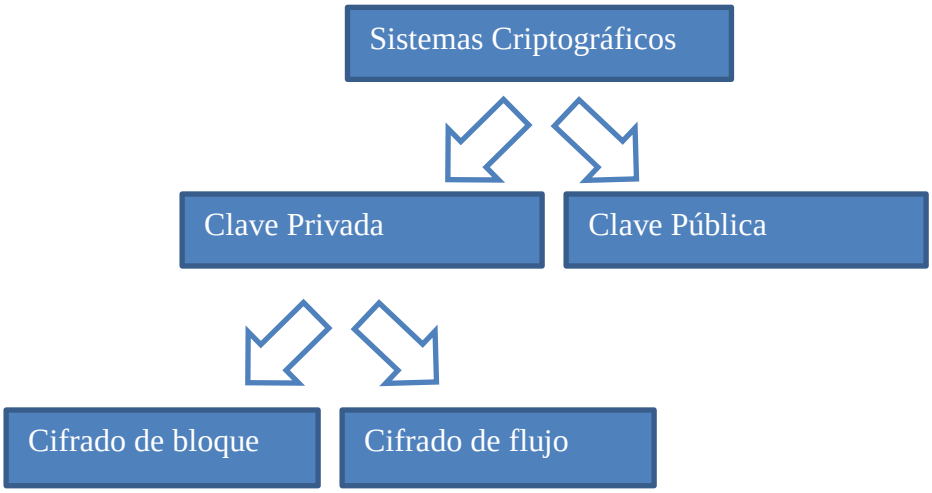

Figura 1 Clasificación de Sistemas Criptográficos

Fuente: Vieites, Sistemas seguros de acceso y transmisión de datos (2014).

2.2.1 Sistemas criptográficos simétricos o de clave secreta

En estos sistemas existe una clave única para el cifrado y descifrado de los datos y la llave es compartida entre todas las partes que deban tener el acceso a los datos. En este caso, la seguridad está en qué tan bien se pueda mantener la clave en secreto.

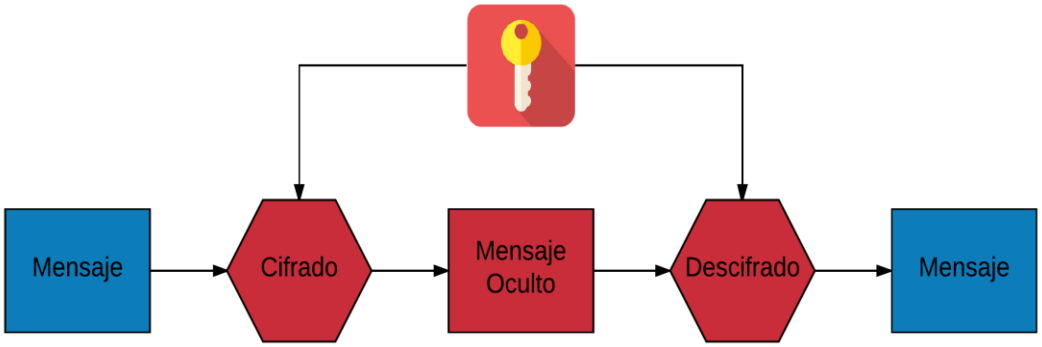

Figura 2 Sistemas criptográficos simétricos o de clave secreta

Fuente: elaboración propia.

2.2.2 Sistemas criptográficos asimétricos o de clave pública

En este tipo de sistemas cada usuario tiene dos claves inversas, una privada y otra pública. Los datos se cifran con la llave privada, el descifrado se lleva a cabo con la clave pública y viceversa. La seguridad de estos sistemas está en la dificultad de invertir la llave pública para encontrar la llave privada.

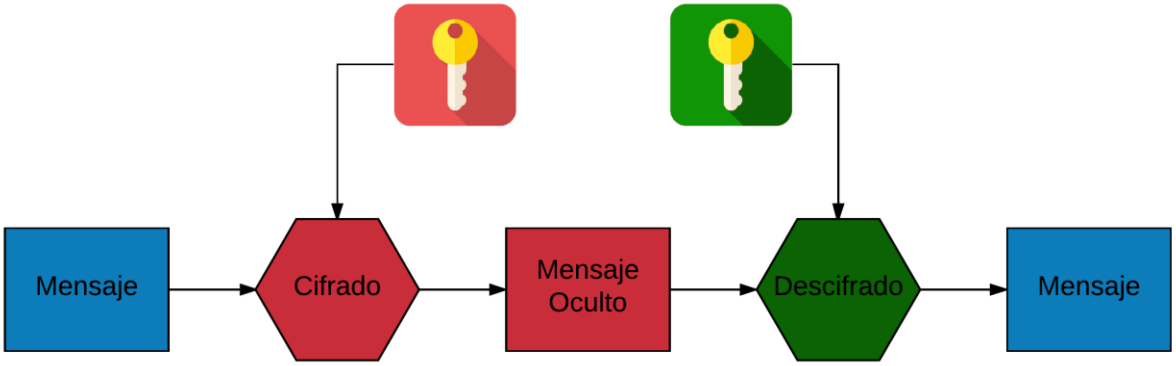

Figura 3 Sistemas criptográficos asimétricos o de clave pública

Fuente: elaboración propia.

2.2.3 Función *HASH*

La función *hash* es un algoritmo que hace un mapeo de los datos originales de tamaño variable en un conjunto de datos de longitud fija.

Las funciones *hash* son de gran importancia ya que garantizan la integridad de los datos, debido a que al cambiar un solo bit de los datos originales el *hash* retornaría un valor diferente al del mensaje original. Se utilizan a manera de cifra de control de los datos originales.

Las propiedades más importantes de las funciones *hash* son:

- Sin importar el tamaño de los datos, el valor del *hash* siempre tendrá la misma longitud.
- Con cambiar un único bit del mensaje original, el valor del *hash* debe ser diferente.
- Resistencia a la pre-imagen, lo cual significa que al tener el valor del *hash* no es computacionalmente posible obtener los datos originales.

- Resistencia a la segunda pre-imagen, esto quiere decir que, si se tiene un conjunto de datos, no sea posible que otro conjunto de datos diferente tenga el mismo valor *hash*.
- Resistencia a colisiones: computacionalmente no es posible encontrar dos conjuntos de datos distintos que den lugar al mismo valor *hash*.

2.3 Firma digital

Está conformada por los datos que se añaden a la información original para que la persona que tenga acceso a esos datos pueda comprobar su origen y su integridad[3], a la vez, también permiten la no repudiación. El proceso es relativamente simple, se toman los datos y se calcula el *hash* de estos, se cifra el *hash* con la llave privada del emisor y se envía con la información original. Si se desea agregar confidencialidad, la información original se puede cifrar con la llave pública de la persona receptora de los datos para que solamente esta pueda descifrar la información original.

La verificación de la integridad del documento firmado es un proceso en el que al documento se le aplica la función de *hash*, luego utiliza la llave pública de la persona que firmó el documento y se descifra la firma digital y se obtiene el *hash* del documento originalmente firmado, luego se compraran ambos resultados y estos deben ser iguales, en caso de que no lo sean se demuestra que el documento ha sido modificado.

[3] En este caso la integridad se refiere a que la información no ha sido modificada desde el momento en que se firmó hasta el momento en que se valida la firma digital.

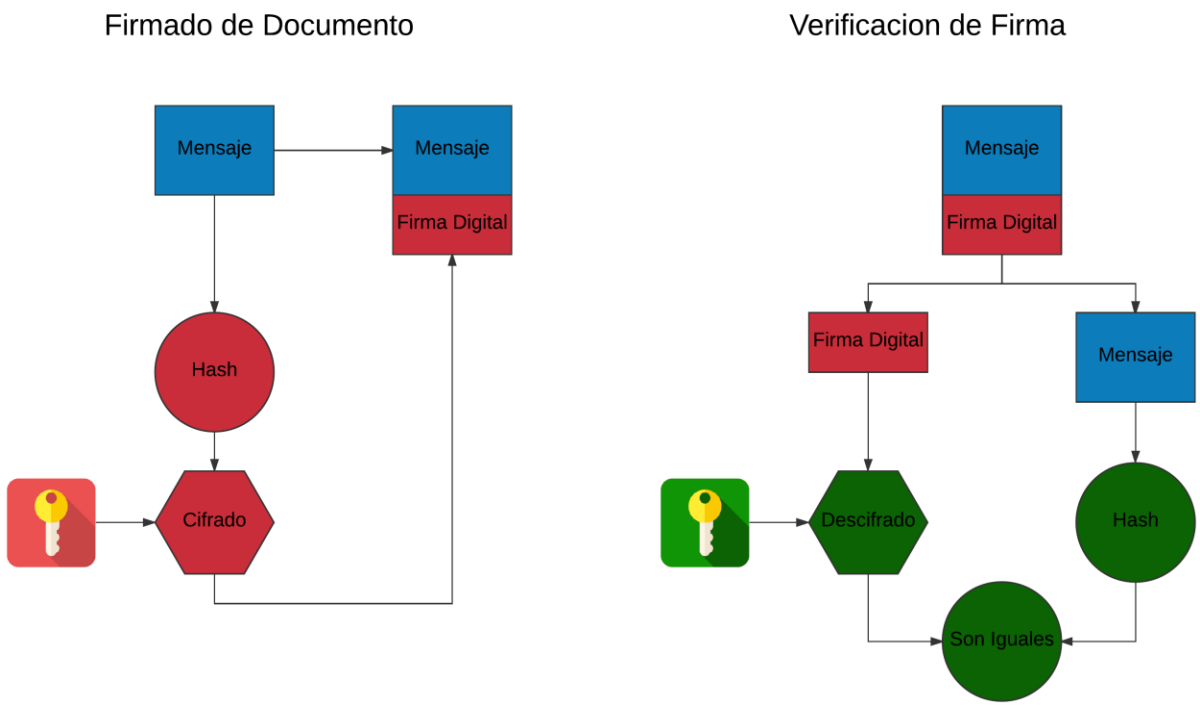

Figura 4 Funcionamiento de la firma digital

Fuente: elaboración propia.

2.4 Firmas ciegas

Las firmas ciegas se diseñaron en los primeros protocolos de dinero electrónico y luego se utilizaron para la validación de los votos en un proceso electoral electrónico. A través del uso de las firmas ciegas se da la posibilidad de que una autoridad firme digitalmente un conjunto de datos, como en este caso un voto, sin conocer el contenido, las firmas digitales ciegas fueron introducidas por Chaum en 1982 (Chaum, 1982).

Un protocolo de firma ciega es un conjunto de algoritmos donde se tiene:

- Un algoritmo de generación de llaves.
- Un algoritmo que convierte el mensaje original en el mensaje oculto.
- Un algoritmo de firmado a ciegas.

- Un algoritmo que revierte el mensaje oculto en el original.
- Un algoritmo que verifica la veracidad de la firma.

Todo protocolo de firma ciega debe tener los siguientes componentes

1. Un protocolo de firma digital de la entidad firmante donde $S(m)$ denote la firma digital del mensaje m.
2. Dos funciones f y g, conocidas solo por el usuario que cumplan

$$g(Sf(m))) = S(m)$$

Este estudio se enfoca en la propuesta de Chaum, dado que la patente de esta propuesta ya expiró y su implementación no significaría un incremento en el costo de la implementación del sistema de votaciones.

El esquema propuesto por Chaum está basado en la firma digital RSA, consiste en que sea $n = p * q$ el producto de dos primos aleatorios suficientemente grandes. El protocolo de firma digital usado por la entidad que firma de forma ciega utilizará un esquema de firma digital RSA con llave pública (n, e) y de llave privada d. Sea k un número entero aleatorio donde $mcd(n, k) = 1$, donde n y k son primos relativos[4]. Las funciones utilizadas por el usuario serían las siguientes:

- $f: m \rightarrow f(m) = m * k^e \ mod \ n$
- $g: m \rightarrow g(m) = k^{-1} * m \ mod \ n$

El protocolo por seguir para la firma ciega sería el siguiente:

[4] Dos números enteros son primos relativos si no tienen ningún factor primo en común, o, dicho de otra manera, si no tienen otro divisor común más que 1 y -1. (Alonso)

1. Fase de Inicialización: sea $0 \leq m \leq n-1$ el mensaje creado por el usuario y que debe firmar la entidad firmante y sea k un entero aleatorio elegido por el usuario tal que $0 \leq k \leq n-1$ y $mcd(k,n) = 1$.
2. Fase de Ocultación: el usuario calcula $m^* = f(m) = m * k^e \ mod \ n$ y se lo envía a la entidad firmante.
3. Fase de Firma: la entidad firmante calcula $s^* = S(m^*) = (m^*)^d \ mod \ n$ y se lo envía de vuelta al usuario
4. Fase de Recuperación: el usuario calcula $s = S(m) = g\big(S(m^*)\big) = k^{-1} * s^* \ mod \ n$, esto es la firma digital del mensaje m generado por el usuario

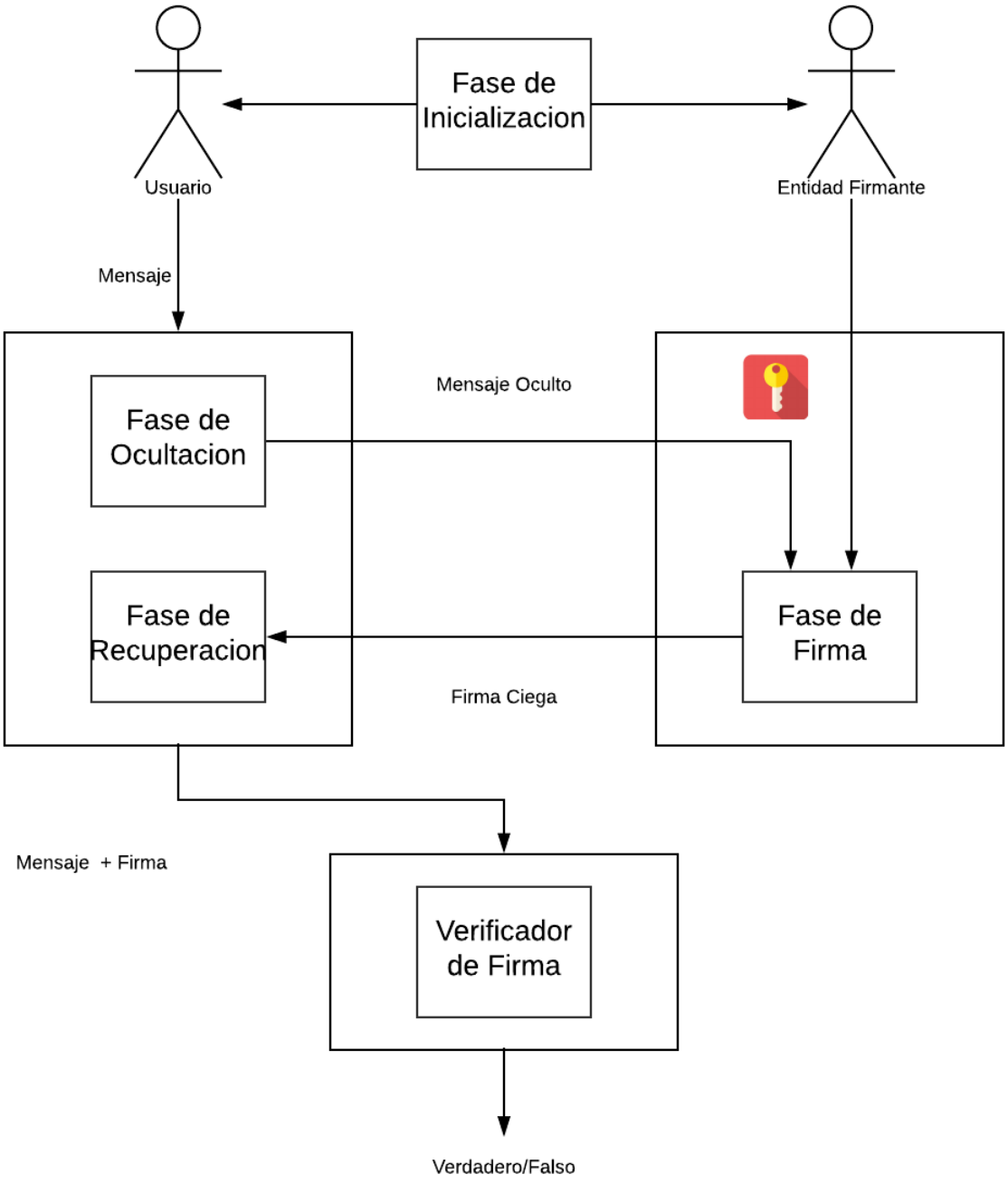

Figura 5 Firma Ciega

Fuente: An efficient blind signature scheme for e-voting system (2015).

2.5 Plataforma *Blockchain*

El *blockchain* se introdujo como un concepto con la invención del Bitcoin en el 2008 que luego se puso en funcionamiento en el 2009.

El *blockchain* es una base de datos compartida que funciona como un libro contable para el registro de transacciones. Está basado en cuatro pilares, los cuales son: el registro compartido de las transacciones, la verificación de las transacciones por medio de un consenso, un contrato virtual en el que se especifica el motivo de la transacción y, finalmente, la criptografía.

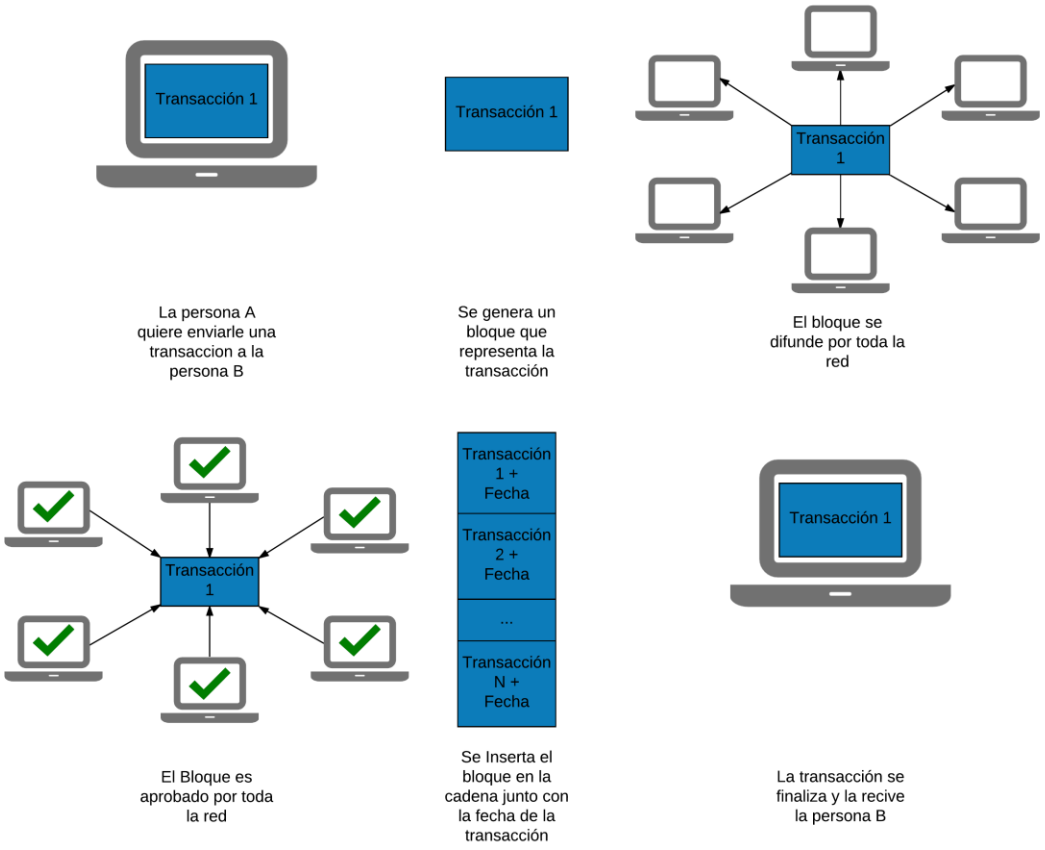

Figura 6 Explicación de funcionamiento del Blockchain

Fuente: DePatie (2016).

Hay muchas plataformas *blockchain* y estas se dividen en 3 tipos dependiendo de los nodos que puede tener acceso a esta, y estos tipos son *Blockchain* pública, *Blockchain* privada y *Blockchain* híbrida.

Blockchain **pública**

Estas son las que son accesibles a cualquier usuario en el mundo. Lo único que se necesita es un dispositivo con conexión a Internet. Debido a esto cualquier persona puede unirse al *blockchain* y participar del proceso de consenso, este es el proceso en el que un bloque se agrega a la cadena y se determina cual es el estado actual de esta, debido a esto los *blockchain* públicos se mantienen seguros gracias a una combinación de dos factores, incentivos económicos y la utilización de mecanismos de consenso como la prueba de trabajo[5] y la prueba de participación[6].

Blockchain **privada**

Es una plataforma de *blockchain* donde se requiere una invitación para ingresar y esta debe ser validada para que un nodo pueda unirse. Esto permite que se pongan restricciones en quien se puede unir a la red, así como los permisos que va a tener dentro de esta. Esto logra que haya participantes que tienen diferentes funciones (permitir nuevas entradas en el *blockchain*, auditoría, dar permisos de participación, etc.) dependiendo de los permisos que tenga.

Blockchain **hibrida**

[5] Prueba de trabajo (*proof of work, PoW*), es un protocolo de consenso, utilizado en redes distribuidas, donde problema matemático-algorítmico que, resuelto, permite a cualquiera de los miembros "mineros" o validadores de la red cerrar el bloque y engarzarlo a la cadena (Jiménez, 2018)

[6] Prueba de Participación (*proof of stake, PoS*) es un protocolo de consenso, utilizado en redes distribuidas, en el que el derecho de acuñar un bloque depende de la participación (cantidad de dinero que el minero posea) (Szmigielski, 2016)

Es el tipo de *blockchain* donde se da algún tipo de combinación entre las dos anteriores, aunque no se logra ver mucha diferencia con las privadas, algunas formas de este tipo son los nodos que proveen el consenso de manera preseleccionada, por ejemplo en un grupo con una cantidad de diez nodos preseleccionados, siete tendrían que aprobar el bloque para que este sea válido, otro tipo sería que los nodos tienen que ser invitados y una vez que el nodo es parte del *blockchain* todas las transacciones son públicas.

Minería de *Blockchain*

Para que el *blockchain* funcione de forma correcta se debe tener un mecanismo que permita la descentralización de forma segura del *blockchain*, a esto se le llama minería. La minería permite que el sistema sea seguro y habilita un sistema sin autoridad central. Esto no se debe confundir con la remuneración o pago a los mineros.

Los mineros son los que validan las transacciones nuevas y las guardan en el *blockchain*. Los mineros compiten por resolver un problema matemático complejo con base en un algoritmo de *hash* criptográfico. Cuando se encuentra un bloque, las transacciones se consideran como confirmadas por lo que la transacción puede proceder. Los mineros en las plataformas de blockchain públicas y en algunos casos de las hibridas reciben una recompensa por resolver este complejo problema matemático.

2.6 Votaciones electrónicas

En los últimos años, con los desarrollos tecnológicos se han migrado procesos manuales a computacionales para así agilizar el proceso y facilitarles el uso a los interesados.

En el caso de las votaciones, estas no han estado exentas de tales transformaciones y se han generado diferentes propuestas para la realización de las votaciones de forma electrónica.

Hay varios tipos de votos electrónicos, entre los que podemos enumerar:

2.6.1 Voto electrónico en papel

En este tipo de votación se tiene de igual forma las papeletas físicas y los votantes seleccionan su candidato realizando un hueco en el papel por medio de algún tipo de dispositivo. Luego se toman las papeletas y se hace el conteo de forma electrónica utilizando las boletas perforadas.

2.6.2 Voto con sistemas de lector ópticos

Este tipo de votación utiliza lectores ópticos para hacer la lectura de las papeletas, el marcado de las papeletas se puede hacer de diferentes maneras las cuales luego las reconoce el lector óptico. Una ventaja es que, al utilizar una papeleta, si el lector óptico falla siempre se tiene la opción de realizar el conteo de forma manual.

2.6.3 Voto electrónico en registro directo DRE

El DRE (*Direct Recording Electronic*) es una votación en la que se ejerce el voto directamente en un dispositivo electrónico que presenta la papeleta electrónica y el votante selecciona el candidato a través de un botón, los cuales se muestran en una pantalla y el voto se graba de forma directa.

2.6.4 Voto por Internet

Este sistema se refiere a las votaciones realizadas a través de Internet, ya sea en un ambiente controlado o no. Con las votaciones por Internet, ni los dispositivos para realizar las votaciones ni el ambiente en el que se manejan los datos se encuentran bajo el control de los encargados de las votaciones.

Este tipo de voto le da la opción a organizaciones de mundiales que no pueden tener votaciones en cada uno de los países donde hay miembros, como por ejemplo IEEE, ISACA.

Capítulo 3. Marco metodológico

Esta investigación abarca los tipos de cadenas de *blockchain* que hay en el mercado, los cuales podrían ser aptos para su uso en un sistema de votaciones a nivel nacional, también la forma como se puede utilizar la firma digital, implementada en Costa Rica, de forma que se asegure el hecho de que solo vota quien puede votar y solamente lo hace una vez y que se garantice el principio de confidencialidad del voto.

3.1 Tipo de investigación

Se realiza una investigación de tipo explicativa, ya que busca demostrar cómo se podría implantar un sistema de votaciones a través de la plataforma de *blockchain* y la utilización de la firma digital en Costa Rica, de forma que se simplifiquen no solo las votaciones en el territorio nacional sino también se pueda hacer fuera del país para la gente que reside en el extranjero, a la vez, también se busca reducir el costo de las elecciones.

3.2 Alcance investigativo

El alcance de este estudio es la definición y explicación de los métodos, técnicas y procedimientos para realizar las votaciones a través de la plataforma de *blockchain* y la utilización de la firma digital en Costa Rica, manteniendo los principios del sufragio: universal, secreto, directo y libre. Así como el cumplimiento de los objetivos que se definieron en el primer capítulo de este documento.

3.3 Enfoque

El enfoque de esta investigación es mixto, ya que se analizan los diferentes tipos de plataformas de *blockchain*, así como los métodos que pueden utilizarse para mantener el anonimato y el control contra el fraude en las votaciones electrónicas.

3.4 Población y muestreo

Se busca la validación de abogados para que analicen la propuesta y se verifique que cumpla con los requisitos de la legislación costarricense.

3.5 Instrumentos de recolección de datos

La recolección de datos se hizo por medio de la búsqueda de información sobre las funcionalidades del *blockchain* y los métodos de uso de la firma digital.

También se analizaron los datos presentados a los abogados y sus recomendaciones.

Capítulo 4. Análisis

Como se mencionó en los capítulos anteriores, en este documento se busca generar una propuesta para un sistema de votaciones electrónico utilizando la firma digital para Costa Rica mediante el uso de la plataforma de *blockchain*.

La plataforma de *blockchain* es en la que se llevará el conteo de los votos y la forma en la que se podrá dar el voto a un candidato en una forma similar a las transferencias financieras de las monedas que se basan en la plataforma *blockchain*. El *blockchain* presenta una plataforma descentralizada y con encriptación en los datos, esto les da la seguridad y la privacidad a los votantes de que los datos no los altera nadie y, a la vez, todas las transacciones son de dominio público y el conteo de los votos sería transparente y en tiempo real.

Para el voto se puede decir que, según se explicó y para cumplir con la legislación costarricense y mantener las cuatro características del voto en Costa Rica (secreto, universal, libre y directo), se necesita utilizar la firma digital, pero también se debe tener en cuenta que esta no debe utilizarse de forma que se pueda hacer una correlación entre la firma y el voto. Para esto se utilizaría el proceso de firmado a ciegas (*Blind Signature*) desarrollado por David Chaum, el cual permite que se realice la transacción dándole el anonimato al votante.

A continuación se analizará de manera general la forma en la que se realiza el voto en este momento en Costa Rica: el Tribunal Supremo de Elecciones (TSE) genera el padrón electoral con la lista de los ciudadanos que cumplen los requisitos para ser votantes hasta el día de las elecciones, para este padrón electoral se deben generar las papeletas para cada uno de los votantes y estas deben enviarse a cada uno de los centros de votación, luego los electores se presentan en los centros electorales, estos se deben identificar utilizando la cédula de identidad vigente ante los fiscales,

los cuales, luego de verificar que la persona es quien dice ser le entregan las papeletas, las cuales están firmadas por al menos 2 fiscales, con las listas de candidatos. La persona pasa a la urna, marca con una X la casilla en las papeletas seleccionando su candidato y luego las deposita en las cajas respectivas, que serán contadas al final del día, después del cierre de los centros de votación y tabular los resultados de las meses y, por agregación, el candidato ganador.

Entonces, ¿cómo se lograría el voto electrónico según la propuesta de este documento?

Para esto se tienen que analizar los requisitos de las votaciones electrónicas, ya que estas tienen un mayor número de vulnerabilidades que las votaciones tradicionales debido a que el procesamiento de los datos podría manipularse y así alterar el resultado de las elecciones. Para reducir estas vulnerabilidades se hace uso de herramientas criptográficas las cuales permiten satisfacer los requerimientos necesarios para las elecciones, a saber:

- Anónimo y habilitar la no coerción: que nadie sea capaz de determinar el valor del voto ni asociarlo con el votante.

- Autenticación: que permita únicamente a los votantes que se encuentran en el padrón electoral ejercer el voto.

- Certificable: el sistema electoral debe ser estable y en el caso de que sea una elección oficial esta debe tener los criterios establecidos por la legislación vigente.

- Confiable: el sistema debe ser robusto, sin fallas en la comunicación y, a la vez, sin pérdida de votos.

- Conveniencia: debe permitir a los votantes ejercer su voto de forma fácil y sin tener conocimiento informático.

- Costo-Eficiente: el sistema de votación debe ser computacionalmente eficiente.

- Exactitud: los votos se deben registrar y procesar de forma correcta.

- Flexible: debe contar con la opción de ser compatible con múltiples plataformas tecnológicas.

- Integridad: los votos no deben poder modificarse, borrarse u omitirse.

- Transparencia: los votantes deben ser capaces de comprender el proceso de votación.

- Unicidad: debe permitir un único voto por votante inscrito en el padrón.

- Verificable y auditable: tiene que permitir que se pueda verificar que los votos se contaron de forma correcta y en su totalidad.

Para lograr esto, lo primero que se definiría sería la plataforma de *blockchain* para realizar las votaciones, debido a que esta permite que se verifiquen, actualicen y mantengan los datos de forma descentralizada, independiente y, a la vez, eliminando los intermediarios, permite proveer una plataforma que a través de los registros digitales cifrados quede como una base de datos compartida en todos los nodos de la plataforma de blockchain, de esta forma, brinda una plataforma idónea para que se almacenen los votos de la elección. Esto, a la vez, permite que el conteo de votos sea de forma automática sin tener que pasar por el registro, administración, conteo y verificación de cada uno de los votos por parte de una autoridad central, ya que el registro de todos los votos estaría en el histórico y no hay forma de modificarlo por una persona, ya que al ser descentralizado todas las versiones en la red deben coincidir, de no ser así se procede a la resolución de conflictos por parte de la plataforma de *blockchain*, la cual ya posee un método para esto.

Por otro lado, ya que se utilizará la plataforma de *blockchain* se debe también tomar en cuenta que al igual que en el resto de las plataformas de *blockchain* la minería tiene una recompensa para el nodo que logra encontrar el siguiente bloque. Para esto se propone que se disponga un porcentaje del dinero que se ahorrará en el cambio a este nuevo formato de votaciones

para dar como recompensa a los nodos de esta forma incentivando la participación de una mayor cantidad de nodos en el proceso para así incrementar la seguridad en la plataforma.

Segundo, para asegurarse que los votos son válidos y que las personas únicamente voten una vez, se utilizaría la firma digital. Esta permitiría verificar la autenticidad y la integridad del voto, lo cual, gracias a la Ley n.º 8454: Ley de Certificados, Firmas Digitales y Documentos Electrónicos, lo convertiría en un documento válido, a la vez, el TSE tiene el proyecto de implantar las cédulas inteligentes, lo cual haría que cada persona que tenga la cédula, a la vez, tenga el certificado digital para poder firmar, aunque de momento este proyecto se encuentra en estudio, de acuerdo con el acta N.º 37-2017 del TSE, una vez que se realice la modificación en la cédula de identidad para que contenga el chip con el certificado digital se puede asegurar que el voto sea universal, debe ser directo ya que al igual que ahora se exigiría la cédula para poder ejercerlo, por lo que de momento solo faltaría garantizar que el voto sea secreto.

Como tercer punto está el firmado a ciegas, como se explicó anteriormente el protocolo de firmas a ciegas permite que se envíe en mensaje de forma anónima sin que se sepa su contenido y, a la vez, se pueda verificar que el mensaje es válido, y de esta manera mantener el voto secreto. La firma ciega funciona de forma que se puede ver como la siguiente analogía: si se toma un papel con el voto y se mete en un sobre de papel carbón sellado con los datos de la persona (firma digital), esta sería la parte de ocultación, el sobre se envía a la entidad firmante y este firma por fuera del sobre de papel carbón, de tal forma que el papel con el voto adentro quedaría firmado sin que la entidad firmante tenga conocimiento alguno del contenido del sobre, esta devuelve el sobre sellado al usuario el cual toma el sobre y saca el papel con el voto y la firma de la entidad, luego coloca el papel en un sobre en blanco sin ninguna información personal y lo envía al destinatario, quien

recibe el sobre sin información de la persona que lo envía, pero al abrirlo puede verificar que es un voto válido ya que contiene la firma de la entidad firmante.

De esta forma, se logra que se mantengan los principios del voto estipulado en la legislación costarricense, de forma que en principio la propuesta es viable para hacer su implementación.

Con respecto al marco legal, se tienen al menos siete categorías de delitos electorales, los cuales no se encuentran tipificados en el código penal ya que estos se encuentran contenidos por la legislación electoral, estas categorías son(Centro de Información Jurídica en línea, 2011):

a- Prevaricato electoral.

b- Delitos contra la imparcialidad y pureza en los comicios electorales.

c- Violación del secreto del voto.

d- Voto múltiple o ilegal.

e- Constricción a la libertad de sufragio.

f- Incumplimiento de las funciones electorales.

g- Delitos relativos a la propaganda electoral.

Para efectos de esta propuesta no todas las categorías aplican o se van a analizar, ya que su relación con la propuesta es poca, por lo que se analizan las siguientes: violación del secreto del voto y voto múltiple o ilegal, las cuales son las que se relacionan directamente con nuestra propuesta.

Con respecto de la violación del secreto del voto contemplado en el artículo 151 inciso a), el cual castiga con pena de dos a doce meses de prisión a “quien violare el secreto del voto ajeno” para este delito, como se explicó anteriormente, gracias a la firma ciega y los algoritmos de cifrado, se permite que el usuario ejerza su voto de forma secreta sin que se tenga algún tipo de trazabilidad de la procedencia del voto o relacionar al votante con su voto.

En cuanto al segundo delito que se analiza en este documento, el cual es el voto múltiple o ilegal contemplado en los artículos 152 y 149 del código electoral, se previenen estos delitos al eliminar la intervención humana, por lo que limita la mayoría de los casos y permite tener trazabilidad, ya que todos los votos pueden ser vistos por cualquier nodo y aunque no se pueda ver quién es el votante, sí se puede auditar y ver si hay algún tipo de fraude y mientras la firma digital del votante sea válida se realizará la firma ciega y se permitirá el voto.

Con respecto de las otras categorías mencionadas anteriormente, estas no aplican de forma directa a lo propuesto en este documento, ya que el alcance de esta no propone una variación a todo el proceso de electoral, sino que se limita al proceso de votación únicamente.

Para las votaciones electrónicas se debería utilizar una plataforma de *blockchain* pública, lo cual permitiría una mayor cantidad de nodos para que, de esta forma, el sistema sea más seguro contra ataques ya que la información se encontraría distribuida en todos los nodos gracias a la descentralización de la plataforma de *blockchain*, además así las votaciones tendrían más transparencia ya que permiten que las transacciones sean auditadas y verificadas por cualquier persona y se puede dar confirmación de que el voto ha sido registrado, si bien es cierto las privadas y las hibridas también dan la mayoría de estos beneficios se podrían dar casos dependiendo de cómo se configuren los permisos donde no toda la información o no todas las transacciones son públicas, además una plataforma privada generaría un costo mayor de implementación dado que los nodos tendrían que ser del TSE y una plataforma hibrida se podría argumentar que está siendo parcializada de alguna forma al limitar los nodos que se pueden unir.

A su vez se recomienda la utilización de la Plataforma de blockchain pública Ethereum por diferentes razones, la primera como se indicó anteriormente es que esta plataforma es publica y robusta dentro de las plataformas de *blockchain* y el costo por transacción bajo, aproximadamente

₡4.54 (aproximadamente $0.008) lo cual significaría que para una votación de 3.6 millones de personas (en el 2018 el padrón electoral fue de 3.322.329) el costo sería de aproximadamente 17 millones de colones, lo cual si lo comparamos con el costo del voto en el 2018 donde únicamente en las papeletas se dio un gasto de 171 millones de colones (Murillo, 2017) , el costo por papeleta en el voto electrónico lo cual sería el costo por la transacción es aproximadamente del diez por ciento. Se elige Ethereum sobre el Bitcoin ya que el costo por transacción es menor, (el costo por transacción en Bitcoin es mucho mayor, aproximadamente de ₡198.5 (aproximadamente $0.35)), además que en la plataforma Ethereum el tiempo de bloque es menor, lo que significa que el tiempo para encontrar la solución para un nuevo bloque toma menos tiempo, también tiene la ventaja de que es escalable y permite el uso de Contratos Inteligentes, esto permitiría que se generen contratos para llevar el conteo de los votos, los cuales serían actualizados cada vez que se ejerce un voto y permiten lleva un mejor control sobre las votaciones.

Tomando en cuenta la información anterior, los siguientes son los requisitos para poder implementar el voto electrónico para esta propuesta:

- La implementación de la cédula inteligente y que toda la población costarricense haga el cambio a esta.
- La aplicación diseñada para el voto electrónico, la cual debe tener como parte de la implementación todas las comunicaciones utilizando SSL/TLS.
- Distribución de dispositivos con lectores de certificado digital y conexión a la red en los centros de votación, estos equipos deben ser configurados de tal forma que queden de tipo *appliance,* o sea que las personas que lo utilicen únicamente puedan realizar los comandos/pasos definidos, así como los puertos deshabilitados.

- Definición del lapso de tiempo en el que los votantes puedan ejercer el voto, dado que el voto se podría realizar desde cualquier lugar del mundo y no se puede definir un rango de horas para cada país la forma más sencilla es que se defina un periodo de tiempo en el que permita a cualquier persona ejercer el voto durante ese periodo por ejemplo veinticuatro horas lo cual sería lo recomendado y la utilización de un servicio de sellado de tiempo[7] para validar que el voto se realizó en el periodo establecido.

El proceso de las votaciones en sí se daría de esta forma sin importar si el votante se presenta a las urnas o si ejerce el voto desde cualquier otro lugar con un dispositivo que cumpla con las características requeridas las cuales serían conexión a la plataforma de *blockchain*, el lector del certificado digital y la aplicación para el voto electrónico.

El proceso comenzaría por el votante obteniendo la papeleta electoral con las opciones definidas y un identificador generado de forma aleatoria en el servidor, una vez que se tiene la papeleta el usuario selecciona la opción por la que quiere votar y luego ocultaría la papeleta marcada con el método definido para el proceso de la firma ciega, y procede a enviarla al TSE firmada con la firma digital, cuando el TSE la recibe valida la firma digital para ver que el votante sea válido (que sea la primera vez que vota, que esté en el padrón electoral, que esté vivo, que el certificado no haya sido revocado, etc.), luego de validar la firma el TSE procedería a firmar la papeleta oculta, para lograr así la firma ciega, y la envía de vuelta al votante, este procede a revertir la papeleta oculta manteniendo la firma del TSE y verificar la firma del TSE y que su opción sea

[7] El servicio de Sellado de Tiempo(TSS) se encarga de recibir la solicitud de sellado de tiempo de un suscriptor, verifica los parámetros de la solicitud y genera el *token* de sellado de tiempo, de acuerdo a las políticas de estampado de tiempo (Ministerio de Ciencia y Tecnología, 2008)

la correcta, y finalmente envía la papeleta con su opción seleccionada y la firma del TSE para ejercer el voto de forma anónima a la plataforma de *blockchain*, en el *blockchain* a través del contrato inteligente[8] (Smart Contract) se valida que la papeleta sea válida y se procede a incrementar el conteo de votos para el candidato seleccionado y se envía el comprobante de la transacción al votante.

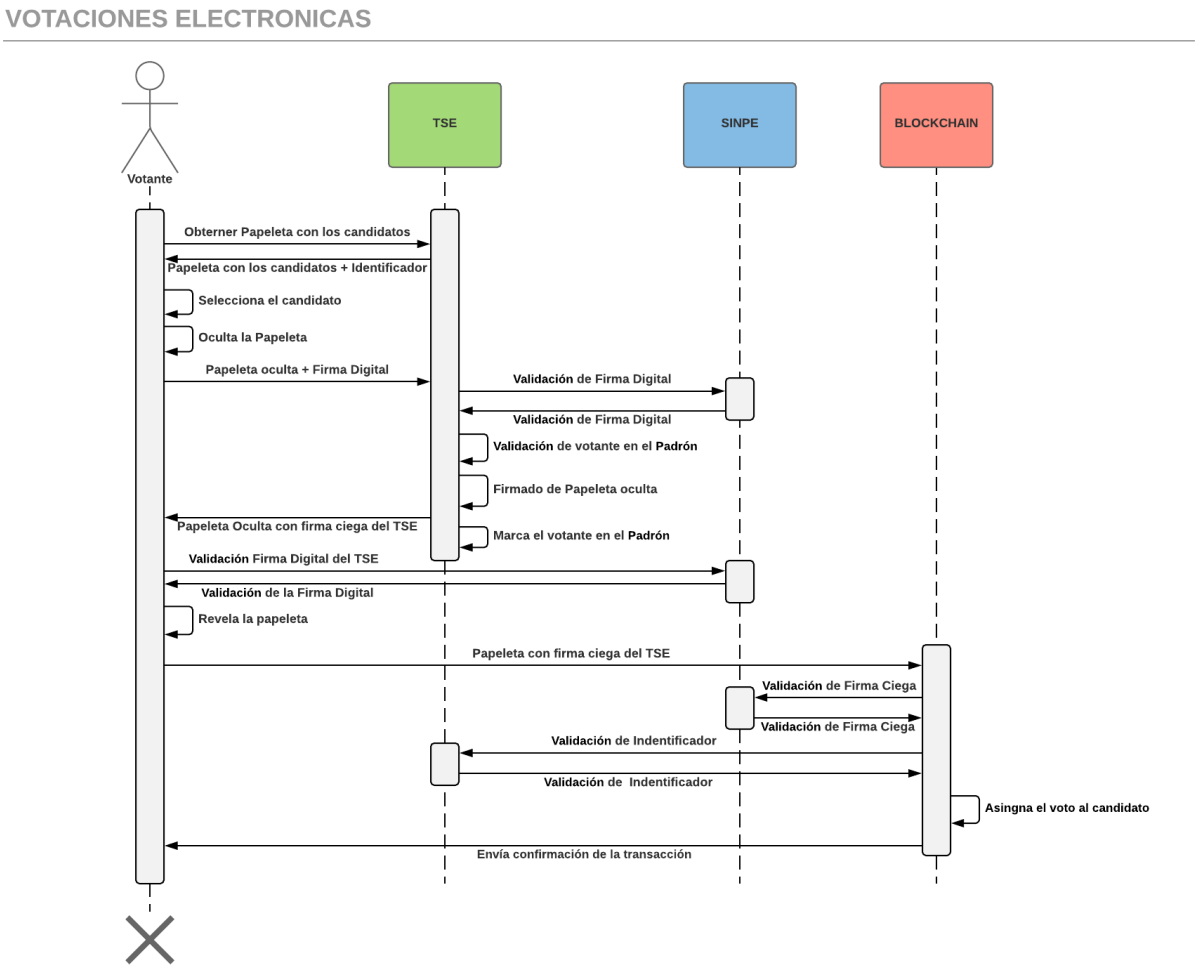

Diagrama 1 Proceso de votaciones electrónicas utilizando la firma ciega y la plataforma de blockchain

Fuente: elaboración propia.

[8] Un contrato inteligente es un programa informático que ejecuta acuerdos establecidos entre dos o más partes haciendo que ciertas acciones sucedan como resultado de que se cumplan una serie de condiciones específicas

Capítulo 5. Conclusiones

Según lo analizado, sería factible la implementación técnica del sistema de votaciones en la plataforma de *blockchain* utilizando la firma digital, debido a que se pueden mantener los cuatro principios del voto costarricense, los cuales son que sea secreto, universal, libre y directo en .

En el área económica esta propuesta es viable, pues no solo permite reducir los costos de las votaciones (las votaciones del 2018 tuvieron un aproximado de ₡220 millones únicamente en la impresión de las papeletas de la primera y segunda vuelta), sino que también reduciría el gasto en la deuda política al eliminar la necesidad de movilizar a los votantes a los centros de votaciones.

En el área legal, según el informe de investigación de la CIJUL titulado *Elecciones o votaciones electrónicas*, legalmente sí se podría implantar un sistema de votaciones electrónicas en Costa Rica, así como cumplir con las recomendaciones hechas en dicho informe en la manera de implantar la propuesta.

La presente propuesta, además, como se pudo ver en el análisis, reduce la posibilidad de fraude electoral, pues cada votante puede verificar que su voto se asignó correctamente al candidato de su elección, además, permite que cualquier persona realice una auditoría de los votos ya que estos están visibles a todos.

Analizando la propuesta se puede notar que existen ciertos servicios de la propuesta donde son vulnerables a un ataque de denegación de servicio (DDOS), estos serían el TSE y el SINPE, por lo que para ese día se debe tener planes de contingencia para poder mantener los servicios arriba de tal forma que las votaciones no se vean afectadas en caso de un ataque de DDOS

Así mismo también debido a que la firma digital requiere de contraseña esto generaría un problema ya que se estima que alrededor de un 40 por ciento de los casos de un departamento de servicio de TI son relacionados a desbloqueo de contraseñas.

Además la complejidad del sistema de votaciones propuesta es alta por lo que el proceso en si sería difícil de entender para la mayoría del electorado, esto generaría resistencia al cambio por parte de los votantes lo cual se tornaría en un mayor porcentaje de abstencionismo.

Bibliografía

Aye, T. y Khin Than, M. (2015). *¿Qué es Bitcoin?* (s.f.). Obtenido de El Bitcoin: https://elbitcoin.org/que-es-un-bitcoin/

Alonso, J. A. (s.f.). *Conjunto de primos relativos*. Obtenido de Exercitium: http://www.glc.us.es/~jalonso/exercitium/conjunto-de-primos-relativos/

An efficient blind signature scheme for e-voting system. (2015). *International Journal of Advanced Computational Engineering and Networking*, 12-18.

Aumenta la cantidad de costarricenses que podrán votar en el extranjero en el 2018. (s.f.). Obtenido de Tribunal Supremo de Elecciones: http://www.tse.go.cr/comunicado400.htm

Bashir, I. (2017). *Mastering Blockchain.* Packt .

Bheemaiah, K. (2017). *The Blockchain Alternative.* Apress.

Blockchain. (s.f.). Obtenido de definicionabc: https://www.definicionabc.com/tecnologia/blockchain.php

Calderon, S. A. (15 de Enero de 2016). *Transporte gratuito el día de las elecciones. ¿Es una necesidad o una ambigüedad?* Recuperado el Octubre de 2017, de Tribunal Supremo de Elecciones: http://www.tse.go.cr/revista/art/22/angulo_calderon.pdf

Centro de Informacion Juridica en Linea. (2011). *Delitos Electorales.*

Centro de Información Jurídica en Línea. (s.f.). *ELECCIONES O VOTACIONES ELECTRONICAS.*

Chaum, D. (1982). *Blind Signatures for untraceable payments.* Obtenido de https://www.chaum.com/publications/Chaum-blind-signatures.PDF

DePatie, J. (s.f.). *New Kid on the Blockchain*. Obtenido de Science and Entertainment Exchange: http://scienceandentertainmentexchange.org/article/new-kid-on-the-blockchain/

Drescher, D. (2017). *Blockchain Basics* (1 ed.). Apress.

Gascó, G. E., Serrano, R. M., & Ramada, D. J. (2013). *Seguridad informática.* Macmillan Iberia, S.A.

Gregersen, E. (s.f.). *Bitcoin*. Obtenido de Enciclopedia Britanica: https://www.britannica.com/topic/Bitcoin

Herrera Loaiza, E., & Villalobos Quirós, E. (2006). SUFRAGIO Y PRINCIPIO DEMOCRÁTICO: CONSIDERACIONES SOBRE SU EXISTENCIA Y VINCULANCIA. *Revista de Derecho Electoral Tribunal Supremo de Elecciones*.

http://www.firmadigital.go.cr. (13 de Octubre de 2005). Obtenido de http://www.firmadigital.go.cr/Documentos/ley%208454.pdf

Humanos, I. I. (2000). Diccionario electoral. (S. edición, Ed.) San José, San José, C.R.

Jayachandran, P. (31 de Mayo de 2017). *The difference between public and private blockchain*. Obtenido de IBM: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Jiménez, J. W. (2018). *Blockchain: primeras cuestiones en el ordenamiento español.* Dykinson.

Lynn, B. (s.f.). Obtenido de https://crypto.stanford.edu/pbc/notes/crypto/voting.html

Madrigal, L. M. (27 de Abril de 2017). *Implementar el voto electrónico en Costa Rica costaría al menos $40 millones de dólares*. Recuperado el Octubre de 2017, de El Mundo: https://www.elmundo.cr/implementar-el-voto-electronico-en-costa-rica-costaria-al-menos-40-millones-de-dolares/

Ministerio de Ciencia y Tecnología. (04 de Setiembre de 2008). Política de sellado de tiempo del Sistema Nacional de Certificación Digital. Obtenido de http://www.firmadigital.go.cr/Documentos/PoliticadeSelladodetiempover100.pdf

Murillo, D. S. (24 de Junio de 2017). *Cada votante en Costa Rica costaría ¢1.459 ($2,5) en las elecciones del 2018*. Recuperado el Noviembre de 2017, de El Financiero: http://www.elfinancierocr.com/economia-y-politica/cada-votante-en-costa-rica-costaria-c-1-459-25-en-las-elecciones-del-2018/A5CKTPKIUNCGJDTQYE5FIJHQ3Q/story/

Oviedo, E. (19 de Junio de 2017). TSE descarta el voto electrónico para el 2018 por su alto costo. *La Nacion*.

Ramírez, A. (18 de Noviembre de 2017). *TSE inició impresión de papeletas para elecciones nacionales*. Obtenido de https://www.crhoy.com/nacionales/tse-inicio-impresion-de-papeletas-para-elecciones-nacionales/

Szmigielski, A. (2016). *Bitcoin Essentials.* Packt Publishing.

TSE. (s.f.). *http://www.tse.go.cr.* Obtenido de http://www.tse.go.cr/pdf/fasciculos_capacitacion/documentos-de-identificacion.pdf

Unidad de Estadística. (2014). *Elecciones Generales En Cifras 1953-2014*. Recuperado el Octubre de 2017, de Tribunal Supremo de Elecciones: http://www.tse.go.cr/pdf/elecciones/eleccionescifras.pdf

Valverde, Z. B. (2010). Recuperado el Octubre de 2017, de Tribunal Supremo de Elecciones: http://www.tse.go.cr/revista/art/9/bou_valverde.pdf

Vieites, Á. G. (2011). *Enciclopedia de la Seguridad Informática.* (2, Ed.) RA-MA S.A.

Vieites, Á. G. (2014). *Sistemas seguros de acceso y transmisión de datos.* RA-MA Editorial.

www.tse.go.cr. (22 de Agosto de 2017). *tribunal Supremo de Elecciones.* Obtenido de http://www.tse.go.cr/concejo/2017/37-2017-del-22-agosto.html?zoom_highlightsub=cedula+inteligente