Electronic Voting Using Blockchain And Smart Contracts: Proof Of Concept

Fáber D. Giraldo, Milton C. Barbosa, y Carlos E. Gamboa

***Abstract*—Blockchain technology has been presented as a support for trust needs between transactions in electronic information systems. Its successful use in cryptocurrencies has allowed it to explore its capabilities in commercial, industrial, and service systems, backed by the operational alternatives offered by Ethereum Smart Contracts and the cryptographic security of public and private key. These keys are used as a way to make online transactions anonymously, with the guarantee offered by the Blockchain network that they are executed safely. With the above in mind, this concept can be extended to the electoral processes, thus allowing its application in electronic voting systems, especially when the protocols currently used lack the trust factor between the different social actors. This document presents a proof of concept in which Blockchain and other technologies are applied, to allow interaction as an electronic voting system for the election of unique candidates. This has been achieved through the specification of an architecture designed especially for electoral processes, from which it is implemented and a simulation is carried out in order to obtain data that generates value, when evaluating Blockchain technology as an alternative to current voting systems.**

***Index Terms*—Blockchain, Cryptography, Electronic Voting, Proof of Concept, Smart Contracts.**

I. Introducción

El ejercicio de realizar elecciones mediante un proceso de votación, ya sea utilizando sistemas de votación convencionales (tarjetas de votación físicas) o sistemas de votación electrónicos, se ha convertido en un evento de mayor relevancia social, además de ser la ruta directa en la que los ciudadanos o miembros de una organización se conectan y se manifiestan con quien los gobierna. Este ejercicio es la fuente y el apoyo de la legitimación entre el gobierno y los gobernados, dando un cierto sentido de estabilidad política en una nación o las diferentes estructuras administrativas que, a través de la democracia, eligen a sus representantes.

Se han propuesto diversas maneras para votar, pasando desde correos, balotas digitales encriptadas, dispositivos de votación, conexiones FTP seguras, tarjetones, autoridades certificadoras, usando biometría, ahora Blockchain, entre otras. Las metodologías tradicionales de votación empleadas actualmente han dado resultado, sin embargo, en diferentes sectores sociales, los resultados electorales se discuten con argumentos que van desde la manipulación del registro de votantes (suplantación, votación de personas no autorizadas), recuento de votos inexacto, fragilidad de seguridad de los sistemas existentes, hasta la imposibilidad de llevar a cabo una auditoría exhaustiva del sistema de votación, para generar la confianza necesaria que estos procesos deben tener [1].

Este documento presenta una propuesta de votación electrónica respaldada por la tecnología Blockchain, cuyo objetivo es satisfacer en gran medida las necesidades expresadas por los actores sociales, combinando procedimientos criptográficos y la programación de acuerdos entre las partes a través de contratos inteligentes (Smart Contracts).

Estos métodos buscan garantizar el cumplimiento de los principios de votación universales, tales como: anonimato, incapacidad para vincular a un votante con el voto, imparcialidad como la incapacidad de conocer resultados parciales hasta el final de la votación, la verificabilidad como la capacidad de verificar la transacción hecha, la fiabilidad e integridad se conoce como la incapacidad de eliminar o cambiar los votos, y la seguridad se entiende como protección contra ataques de denegación de servicio o pérdida de información [2].

Este artículo está organizado de la siguiente forma. La Sección II presenta el contexto del escenario de votación empleado en la prueba arquitectónica. La Sección III habla sobre el planteamiento del problema. La Sección IV describe la prueba arquitectónica implementada. La Sección V presenta los resultados obtenidos así como una discusión respecto a la aplicabilidad de la técnica en el contexto electoral propuesto. Finalmente, se presentan las conclusiones y trabajos futuros.

II. Contexto

Esta prueba de concepto se abordó con el propósito de satisfacer los principios universales de los sistemas de votación, y en especial los de fiabilidad e integridad, por lo que en este apartado se presentan los conceptos principales de los sistemas de votación, y de las tecnologías utilizadas en la Blockchain.

A. Consulta de Opinión (Universidad del Quindío)

Una consulta de opinión es un proceso mediante el cual se puede elegir las diferentes directivas académicas de la Universidad. Este proceso permite al personal administrativo, docentes, y estudiantes habilitados dar su voto a un candidato, en este caso particular, a un candidato que aspira al cargo de Rector de la Universidad del Quindío.

Cuando un elector desea votar, busca su nombre en los listados en papel que dispone la Universidad para conocer su

F. Giraldo, profesor e investigador del grupo de Sistemas de Información y Control Industrial (SINFOCI) en el Centro de Estudios e Investigaciones de la Facultad de Ingeniería (CEIFI) de la Universidad del Quindío, Armenia, 630004 Colombia, email: fdgiraldo@uniquindio.edu.co.

M.C. Barbosa estudiante del Programa de Posgrado de Maestría en Ingeniería de la Universidad del Quindío, Armenia, 630004 Colombia, email: mcbarbosat@uqvirtual.edu.co.

C.E. Gamboa estudiante del Programa de Pregrado de Ingeniería de Sistemas y Computación en la Universidad del Quindío, Armenia, 630004 Colombia, email: cegamboam@uqvirtual.edu.co.

Manuscrito recibido el Diciembre 1, 2019; revisado XXX.

lugar y mesa de votación dentro del Campus Universitario, posteriormente se acerca a la mesa, se identifica con un documento de identidad, para recibir un tarjetón con el cual llega a un cubículo donde puede ejercer su voto de forma anónima. Finalmente su voto es depositado en una urna.

B. Voto Electrónico

Es el sistema más avanzado dentro de los sistemas de democracia electrónica, ya que es 100% digital, desde la autenticación del ciudadano hasta la emisión del sufragio [3]. Existen 2 tipos de voto electrónico [1], el primero se da cuando el elector está presente en su puesto de votación y el segundo cuando es realizado usando internet en cualquier ubicación.

Para el presente trabajo se parte de la presunción de que el proceso electoral, se hará con la utilización de mesas de votación ubicadas físicamente en un puesto de votación, que será desde donde el ciudadano emitirá un voto a favor del candidato de su preferencia.

Las formas de votación electrónica van desde el uso de tarjetas perforadas, sistemas de escaneo óptico y sistemas de votación Electrónica de Grabación Directa (DRE en inglés) hasta boletas a través de internet y votos telefónicos [4]. Sin embargo, todos tenían algo en común, los diferentes principios que se deben tener en cuenta para que una votación se haga de forma satisfactoria. Según [5] se deben tener en cuenta los siguientes: elegibilidad, no reusable, anonimidad, exactitud, sin juicios parciales, público, verificable, e integridad.

C. Trabajos Anteriores

El trabajo [6] propone un sistema que permite realizar un proceso electoral, donde los electores pueden emitir tokens desde su billetera, a un candidato; previa validación de su identidad por los administradores. Además, usan una prueba de conocimiento cero para validar la boleta de votación emitida.

En [7] proponen emplear IoT para autenticar al votante y posteriormente enviar su voto a la blockchain, que es donde finalmente permanece almacenado. Una vez terminada la jornada electoral, inician el conteo de votos y emiten el ganador. En [7] se afirma que esto se logra a un costo más bajo en comparación con la votación tradicional en papel.

Cada vez la tecnología Blockchain atrae más miradas para ser usada en el voto electrónico, y esto se puede ver en [8], el cual analiza 15 trabajos de diferentes enfoques en pro del voto electrónico. La mayoría coinciden en que Ethereum es una tecnología prometedora para este tipo de eventos, y la usan de diversas maneras. Para hacer una comparativa de estos trabajos, los autores se basan en los siguientes parámetros tales como: autenticación, plataforma, anonimidad, verificación del votante, descentralizado y tecnología usada [8].

Hay países que han implementado este sistema, entre ellos están: Bélgica, Brasil, Estados Unidos, Estonia, Filipinas, India, y Venezuela [2]. Unos están en proceso de implantación y otros la evitan, como Alemania, Holanda, Finlanda, Irlanda, Kazajistán, Noruega, y Reino Unido [2].

En [9] muestran un sistema de votación llamado BroncoVote para universidades usando Ethereum y sus Smart Contracts, que les permite administrar los votantes y la trazabilidad de votos.

De los países mencionados, Estonia decidió implantar el voto electrónico mediante un sistema llamado I-Voting, el cual permite a todos sus habitantes votar desde cualquier rincón del mundo y cambiando de elección de candidato si el votante así lo desea, donde el último candidado que se haya seleccionado, será a quien se le cuente su voto [10]. I-Voting fue recibido con escepticismo, ahora goza de gran popularidad y cada vez va en aumento, hasta alcanzar un tiempo medio de voto por Internet en 2015 de 2 minutos y 36 segundos, que fue calculado teniendo presente que la jornada electoral dura toda una semana (del 21 al 27 de febrero) [10]. Bolivia es uno de los muchos países que continúan realizando votaciones de la forma tradicional con tarjetones físicos, mesas de votación en un lugar específico, jurados y electores; teniendo los mismos problemas que otros países: fraude electoral, errores humanos en los procesos, vulneración a ataques informáticos, proceso electoral centralizado por Entidades autónomas, entre otros [11]. En [11] se realiza una propuesta de voto electrónico para Bolivia usando una billetera y monedas como un activo para votar, por lo que el elector envía una moneda al candidato de su preferencia como una forma de voto [11].

Frente a la viabilidad o no de esta tecnología, se continúa investigando y proponiendo ideas, entre las cuales se tienen: entidades certificadoras, votos firmados digitalmente para comprobar su origen, sesiones FTP (File Transfer Protocol) seguras, algoritmos de encriptación simétrica, entre otros.

D. Blockchain

Esta tecnología es empleada para construir tipos específicos de bases de datos distribuidas compuestas de bloques de datos inmutables, cada uno con una lista de transacciones y una referencia única a su bloque predecesor. La tecnología Blockchain es objeto de una atención intensa y creciente entre los gobiernos [12]. Para poder realizar referencias a bloques anteriores se usan relaciones matemáticas de hashes, siendo la base de datos protegida criptográficamente y gestionada por una red global de computadores, donde la información almacenada no puede ser alterada [13].

La red Blockchain vio la luz en el año 2008 de forma teórica y en el 2009 se implementó una para Bitcoin. La teoría de la misma fue dada a conocer por el seudónimo Satoshi Nakamoto a través del Whitepaper reportado en [12].

Dentro de una Blockchain, todo es un nodo. Un nodo hace referencia a una persona que, a través de un computador, con una copia local de la red y un software especial para minar, entra a formar parte de la red. Esta persona se encarga de hacer minería de bloques, velar por la integridad y transparencia de la red, al participar de un mecanismo llamado consenso.

Todas las actualizaciones de los estados de la Blockchain se realizan a través de transacciones, empleando criptografía de llave pública y privada. Estas transacciones generan un costo medido en gas, el cual es una medida del gasto computacional por parte de los mineros para poder escribir en la red. La cantidad de gas empleado en una transacción, es quien determina la recompensa para los mineros.

Este gas además de ser el estímulo económico para la participación de los mineros en la red, también puede ser usado

en la prevención de ataques sobre la red, dado que, para enviar muchas transacciones con la finalidad de generar un ataque de denegación de servicios, sería costoso para el atacante, pues cada vez que realice un ataque significa un consumo de gas que tiene un valor monetario real. La seguridad de la red es directamente proporcional a la cantidad de mineros activos, por lo que estos la gestionan y ayudan a prevenir ataques como el del 51%, donde un minero se hace con el 51% del poder computacional de la red, y podría manipularla a voluntad [13].

E. Ethereum

Desarrollada por Vitalik Buterin, Ethereum es una plataforma abierta de Blockchain que permite a cualquiera crear y usar Aplicaciones Descentralizadas (DApp en inglés) que se ejecutan en la tecnología Blockchain [14].

El código en Ethereum es ejecutado dentro de una máquina virtual llamada Máquina Virtual de Ethereum (EVM por sus siglas en inglés). Esta puede ejecutar código de complejidad algorítmica arbitraria, por lo que los desarrolladores pueden crear aplicaciones descentralizadas que funcionan en la EVM, esto se hace usando lenguajes programación conocidos, como JavaScript y Python [14].

Los contratos están programados en Solidity el lenguaje más popular. Éstos son una colección de estados y funciones, similares a una clase de Programación Orientada a Objetos [15]. Cuando los contratos son desplegados, se les asigna una dirección para llamar las diferentes funciones públicas propias, que representan la lógica de negocio en una DApp.

Una dirección (clave), es una secuencia de caracteres que representa una cuenta dentro de la Blockchain, usando la criptografía basada en el Algoritmo de Firma Digital de Curva Elíptica (ECDSA), se genera una clave pública y una privada, donde la primera puede ser conocida por cualquiera, la privada es de uso personal para gestionar activos o Tokens. La dirección pública es obtenida a partir de la dirección privada, y no se puede realizar el proceso contrario.

Un token es una representación de un valor financiero o un activo digital que puede ser usado por los diferentes usuarios de la red, para intercambiarlo mediante transacciones.

F. Tecnologías Usadas

En la prueba de concepto se utilizaron las siguientes:

- *Ganache*: la cual simula una Blockchain privada, similar a la red principal de Ethereum que es pública.
- *Metamask*: un plugin que permite a un navegador, trabajar con estas tecnologías descentralizadas.
- *Truffle*: una suite de desarrollo para contratos inteligentes, la cual tiene un depurador, compilador, y comandos para desplegar Smart Contracts.
- *ReactJS* y *JavaScript*: librería y lenguaje de programación respectivamente, usadas para el FrontEnd.
- *Web3JS*: una librería mediante la cual se puede conectar el FrontEnd con los Smart Contracts almacenados en la Blockchain y llamar sus funciones.

Se elige la Blockchain de Ethereum, dado que permite la programación de contratos inteligentes para la lógica de negocio, permitiendo la creación de tokens personalizables, además, se considera que es una Blockchain estable, la cual tiene una gran acogida por su flexibilidad, y se espera que tenga soporte por mucho tiempo. Se descarta la red de Bitcoin dado su enfoque de alta transparencia que puede ser perjudicial para la anonimidad, cayendo en los inconvenientes que se describen en la siguiente sección. Además, no se tiene control alguno sobre la misma. Cardano se descarta porque la introducción de contratos inteligentes es reciente y podrían contener errores, igual sucede con otras blockchains.

III. Planteamiento del Problema

La forma tradicional de voto usando tarjetones, como un mecanismo de participación, recibe duras críticas por la poca transparencia y su elevada complejidad para auditar los votos emitidos. Sumándose a esto, la desconfianza de los electores dadas las garantías de integridad, fiabilidad y anonimato, va en aumento, dado que el sistema se presta para que se cuenten votos a favor de un candidato, mediante los terceros que interactúan en el escrutinio. Además, algunas propuestas encontradas, como se describe en la siguiente sección, abordan mayormente alguno de estos principios, dejando de lado otros. Razón por la cual, se hace necesario una solución que permita hacer frente a estas necesidades.

IV. Solución

A diferencia de otras propuestas, el presente elimina la necesidad de terceros (como autoridades certificadoras), también la posible coacción a los electores, y el exponer una clave pública ligada al voto cuando se realiza la transacción; inconvenientes que en la mayoría de la literatura no profundizan. La propuesta viene sustentada sobre el estándar ERC-20 (Solicitud de Comentarios de Ethereum). Este permite crear tokens y, en este caso particular, usarlos a modo de voto. Cabe aclarar que se ha modificado sutilmente el comportamiento de las funciones del token con la finalidad de adaptarlo al proyecto; particularmente, la forma en que se consulta los balances de las cuentas de los candidatos, para cumplir con el criterio de imparcialidad. Los autores en [16] proponen una forma similar de voto pero usando monedas, donde a cada votante se le asigna una y podrá enviarla a la billetera del candidato como apoyo, desde cualquier lugar y dispositivo que soporte las tecnologías analizadas. Este método es fácil y rápido, sin embargo, se corre el riesgo de dar con la identidad del votante, dado que el elector usa su clave pública para votar quedando registrada en la transacción, y a su vez, se encontraría ligada a la billetera del candidato; por lo tanto, cualquiera que conozca esa clave podrá saber por quién ha votado esa persona. Otro inconveniente es la coacción para revelar su clave pública, y así, buscar entre las transacciones de la blockchain hasta dar con la transacción del voto. Finalmente, otro punto a destacar es el trabajo adicional entregado al votante, dado que debe recordar la dirección privada para poder votar, y, si la pierde, no podría hacerlo. En esta propuesta que se presenta, se usa únicamente la dirección de la mesa y la del candidato para hacer transferencias de tokens en lugar de monedas, con lo cual se supera los anteriores inconvenientes

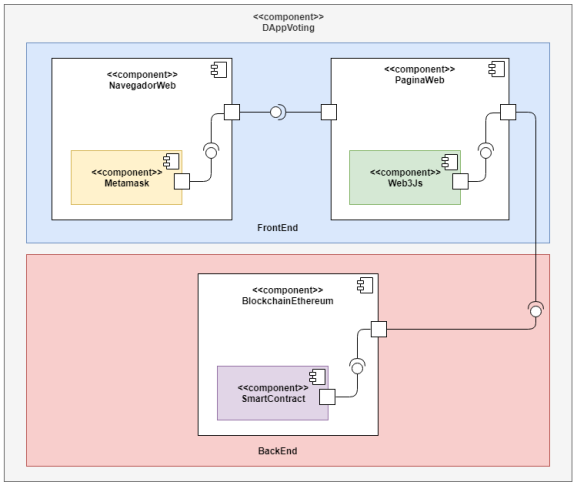

Fig. 1. Arquitectura desacoplada del proyecto.

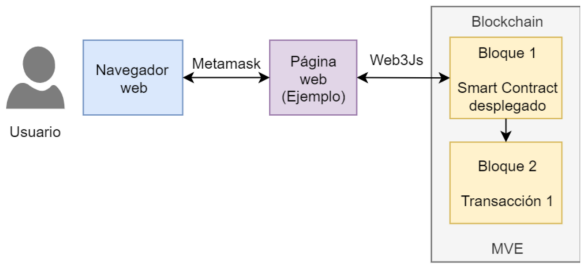

Fig. 2. Interacción de un usuario con la aplicación.

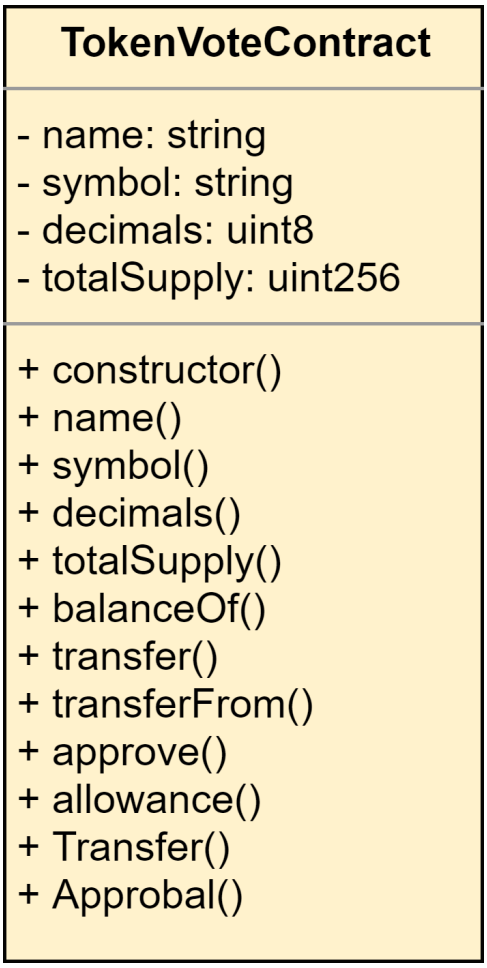

Fig. 3. Ejemplo de Smart Contract TokenVoteContract empleado para almacenar los votos (tokens) de los candidatos.

de anomidad, al no tener una dirección sobre la cual relacionar al elector con su voto. Para iniciar, se crean tantos tokens como electores potenciales estén habilitados, y se transfiere una cantidad determinada de estos a las mesas, en base al número de votantes que hayan sido asignados a la misma usando listas de papel. Esto se hace con la finalidad de que cada mesa sea quien autentique y autorice a sus electores a gastar tokens que le fueron transferidos; por lo tanto, el elector es libre para gastar (emitir) un único token (voto) en nombre de la mesa, por lo que puede transferirlo a la cuenta del candidato como un símbolo de apoyo (voto). Como consecuencia, se puede realizar la trazabilidad de los datos, dado que la granularidad es simple, y además, permite la anonimidad del votante, puesto que únicamente se vincula a la mesa con el voto emitido y el candidato receptor.

A. Diseño Arquitectónico

Dentro del diseño se emplearon 2 patrones arquitectónicos, el usado por la red Blockchain y el patrón Model View View-Model (MVVM). El primer patrón será el modelo (Model) del segundo para almacenar datos de la DApp. La vista (View) está dada por las interfaces de usuario empleadas para presentar la información al usuario, y el ViewModel corresponde a los contratos, donde se programará toda la lógica de negocio.

Con el fin de conocer cómo se relacionan los diferentes componentes del sistema que se está desarrollando, se presenta un diagrama de componentes para ver las diferentes interrelaciones, tal y como se puede apreciar en la Figura 1. Esta se explica con mayor facilidad empleando la Figura 2, que es una abstracción de la Figura 1.

Ambas figuras muestran cómo se trabaja el flujo de los datos, teniendo presente dónde se originan, mediante las acciones de un usuario, y dónde terminan almacenados, que es en la Blockchain de Ethereum.

Ahora que se tienen modelados los datos, se procede a seguir con la arquitectura. En este caso corresponde trabajar con el ViewModel, empezando por los contratos inteligentes.

Los diferentes contratos inteligentes implementados se pueden visualizar en las Figuras 3 a 5. Estos son los que harán las veces de ViewModel dentro del patrón arquitectónico MVVM. Esta lógica puede ser programada usando algún lenguaje que pueda ser interpretado por la EVM.

Antes de continuar, se aclara lo siguiente: se tienen 3 tipos de contratos y 3 tipos de actores. El primer actor es el representante del Consejo Electoral y se encarga de usar el contrato ElectoralProcessContract; el segundo es el representante de los jurados de la mesa, el cual interactúa con el contrato VotingTableContract durante la jornada electoral, y el tercero es el votante, que también usa este último contrato.

Se propone que cada una de las mesas ubicadas en localizaciones específicas, tenga a su disposición un Smart Contract

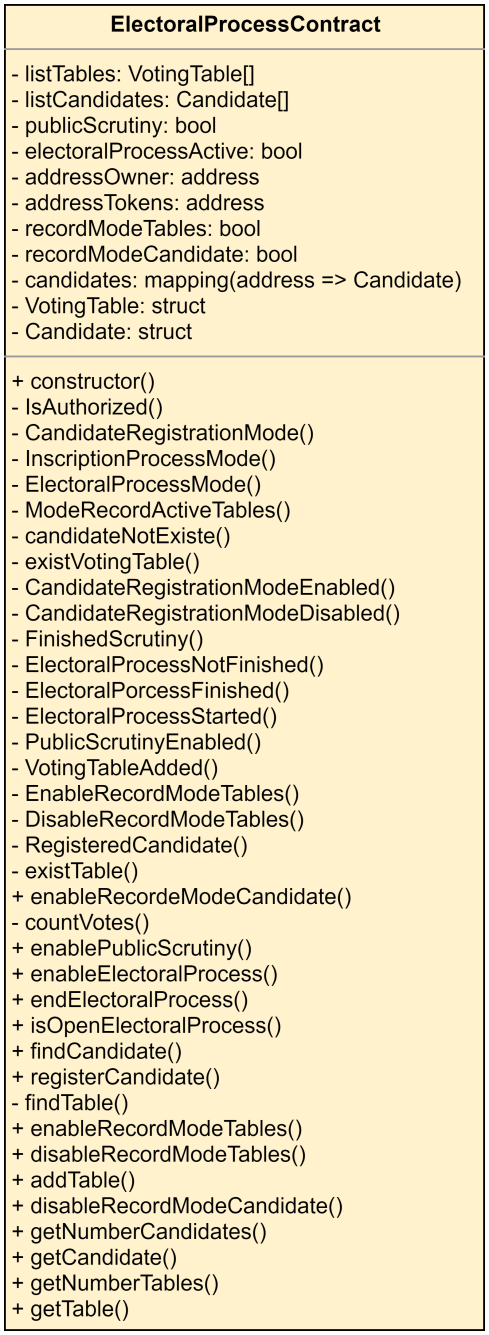

Fig. 4. Smart Contract ElectoralProcessContract empleado para gestionar el proceso electoral.

(*VotingTableContract*) mediante el cual se podrá comunicar con un contrato principal (*ElectoralProcessContract*) controlado por la Entidad encargada del monitoreo del proceso electoral, y a su vez, estos podrán comunicarse con un tercer contrato llamado *TokenVoteContract*. El contrato *ElectoralProcessContract* gestionará lo relacionado con la configuración inicial del proceso electoral (creación de mesas de votación, candidatos, autorización para inicio y cierre de las votaciones, habilitar el escrutinio público) siendo usado únicamente por la persona que sea designada por el Consejo Electoral. Las mesas y los electores podrán usar el contrato *VotingTableContract* para autorizar votos y votar, respectivamente. *TokenVoteContract*, tendrá un registro de los balances (cantidad de votos) de cada de una de las cuentas de los diferentes candidatos y mesas habilitadas, durante el desarrollo de la jornada electoral.

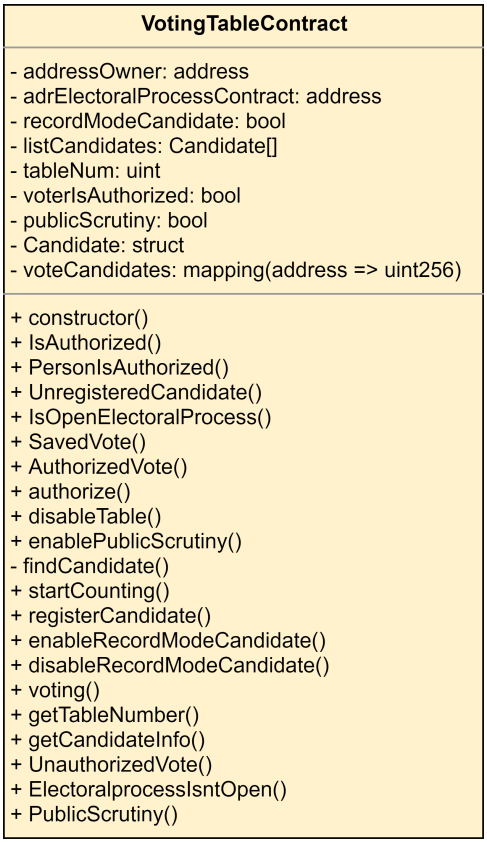

Fig. 5. Smart Contract VotingTableContract, empleado para autorizar y emitir votos.

Las ventajas que ofrecen los Smart Contracts y la Blockchain de Ethereum, es la posibilidad de realizar operaciones transaccionales que son atómicas, es decir, se realiza una transacción completamente o la EVM revierte los cambios si ocurre algún problema. Esto también se puede realizar manualmente, para deshacer cambios cuando hay intentos de fraude detectados en el consenso. Otra ventaja es la suscripción a eventos que están ocurriendo en los Smart Contracts, por ejemplo, emitir una alerta de cuando se activa el proceso electoral, haciendo que esta llegue a algún FrontEnd o dispositivo, con la finalidad de mitigar intentos de fraude. Finalmente, se puede configurar a los Smart Contracts para que únicamente acepten conexiones desde un dominio de red específico, en este caso particular, los puestos de votación.

B. Aplicación Descentralizada o DApp

Como resultado del diseño planteado en las secciones anteriores, se logra el desarrollo de la aplicación presentada en las Figuras 6 y 7.

En el material complementario que se relaciona en la Sección VI, se puede visualizar los diferentes roles que forman parte del proceso electoral, como también las opciones para consultar los resultados finales, o por mesa dependiendo del caso. Mediante la página web de la Figura 6, el elector podrá

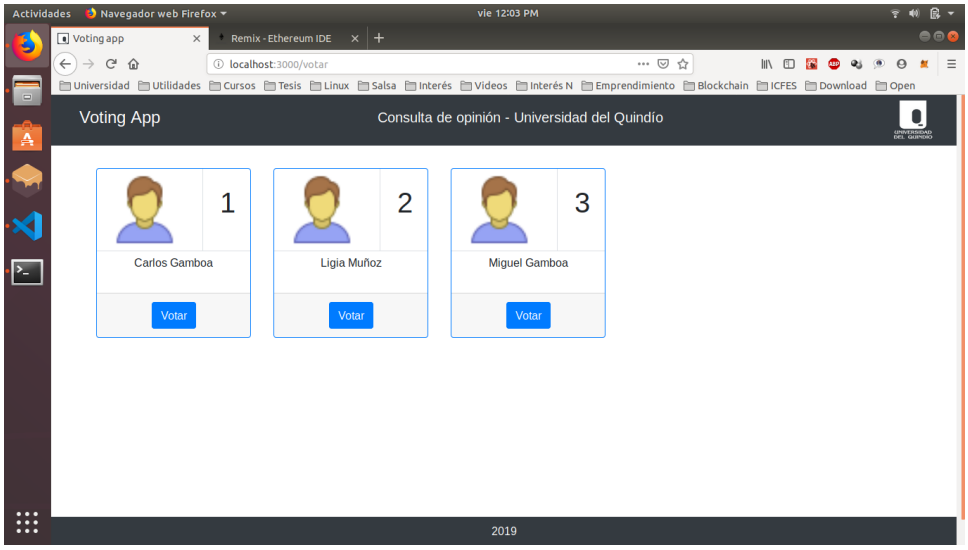

Fig. 6. Interfaz empleada por el votante para emitir su voto en apoyo a un candidato de su preferencia.

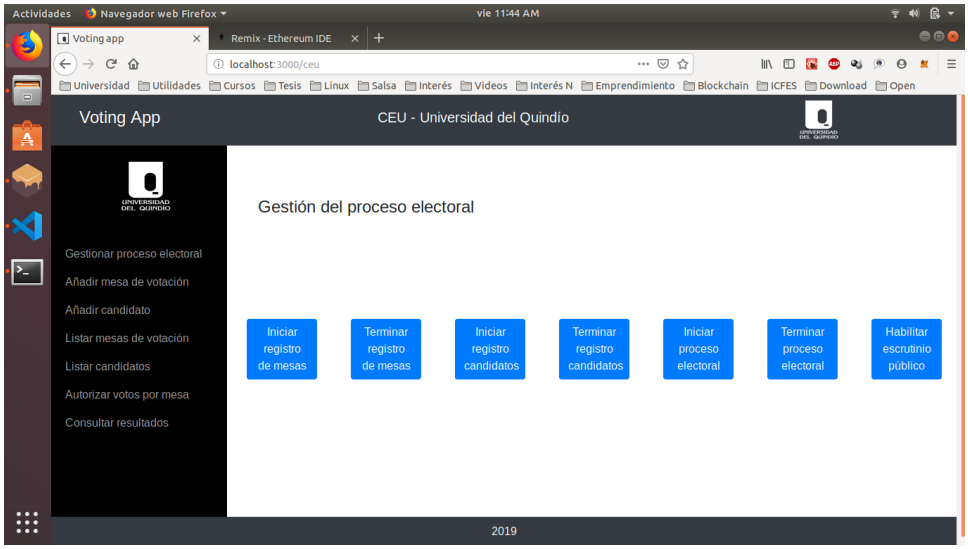

Fig. 7. Interfaz para la gestión de una jornada electoral por parte del representante del Consejo Electoral.

elegir su candidato de preferencia, y una vez la mesa autorice su voto, podrá enviarlo como apoyo al candidato elegido. Esta autorización se da a través de otra interfaz empleando un botón de *Autorizar voto*, una funcionalidad que le permite al elector gastar un token del saldo de la mesa y enviarlo a un candidato a modo de apoyo. A través de la Figura 7, se tendrá un control total sobre el proceso electoral, permitiendo gestionarlo. Una vez ha concluido la jornada electoral, se dispone de una página pública, donde cualquier interesado podrá conocer los resultados del proceso electoral. Esto también se puede hacer empleando otra de las páginas que se implementa, habilitando consultas de los votos que obtuvo cada candidato por mesa, con el fin de comprobar los resultados finales, cumpliendo con el principio de público y verificable.

V. Resultados y Discusión

Empleando la prueba de concepto como punto de partida para tener datos fiables, y así emitir juicios acertados al evaluar dichas tecnologías en secciones posteriores, se realiza una tabla en la cual se presenta los diferentes gastos en cuanto a gas y ether (conocida como ETH), siedo esta última la moneda oficial de Ethereum; al momento de hacer cada una de las transacciones, y así, tener un valor aproximado de cuánto puede costar cada una de estas.

Como se ha indicado, el gas representa el costo computacional requerido para ejecutar una transacción y ser agregada a la Blockchain, dicho costo permite establecer el valor económico de ejecutar cada función de un Smart Contract. La Tabla I presenta los costos asociados a cada una de las funciones de los contratos usados en la prueba de concepto.

Es importante tener cuidado con el costo computacional (gas) dado que no es lo mismo que el costo económico (ETH), pues el costo computacional es fijo mientras el costo económico es variable, y se acoge a la fluctuación como cualquier otra moneda. Por ejemplo desplegar el contrato

TABLA I
LISTA DE COSTOS POR TRANSACCIONES Y CONSULTAS.

Descripción	Costo (gas)	Costo (ETH)
Desplegando contrato Migrations	284908	0,0056982
Desplegando contrato TokenVoteContract	1352345	0,0270469
Desplegando contrato ElectoralProcessContract	2765819	0,5531638
Desplegando contrato VotingTableContract	1974552	0,03949104
Habilitando registro de mesas	29797	0,000596
Registrando mesa 1	86978	0,00174
Terminando registro de mesas	28997	0,00058
Iniciando registro de candidatos	33203	0,000664
Registrando candidato 1	199437	0,003989
Registrando candidato 2	170183	0,003417
Registrando candidato 3	172117	0,003442
Terminando registro de candidatos	32601	0,000652
Autorizando tokens para la mesa 1	51289	0,001026
Listando mesas de votación	0	0
Listando candidatos	0	0
Iniciando Consulta de opinión	29397	0,000588
Autorizando voto para el elector	46528	0,000931
Votando	41459	0,000829
Terminando Consulta de opinión	110690	0,002214
Habilitando escrutinio público	55304	0,001106
Consultando resultados (Consejo Electoral Universitario CEU)	0	0
Consultando resultados (público)	0	0
Auditando mesa 1	0	0
Totales	7465604	0,6471739

TABLA II
FÓRMULAS PARA EL CÁLCULO DE COSTOS.

Transacción	Fórmula
Despliegue del contrato *Migrations*	c_m: costo de desplegar el contrato $c_m = e * p$
Despliegue del contrato *TokenVoteContract*	c_t: costo de desplegar el contrato $c_t = e * p$
Despliegue del contrato *ElectoralProcessContract*	c_e: costo de desplegar el contrato $c_e = e * p$
Despliegue de los contratos *VotingTableContract*	c_v : costo de desplegar el contrato n: cantidad de mesas de votación $c_v = e * p * n$
Habilitar registro de mesas de votación	c_{hm} : costo de habilitar registro de mesas $c_{hm} = e * p$
Registro de mesas de votación	c_{rm}: costo de registrar las mesas n : cantidad de mesas $c_{rm} = e * p * n$
Terminar registro de mesas de votación	c_{tm}: costo de terminar registro de mesas $c_{tm} = e * p$
Habilitar registro de candidatos	c_{hc}: costo de habilitar registro de candidatos $c_{hc} = e * p$
Registro de candidatos	c_c: costo de registrar los candidatos n : cantidad de candidatos $c_c = e * n * p$
Terminar registro de candidatos	c_{tc}: costo de terminar registro de candidatos $c_{tc} = e * p$
Transferencia de tokens a las mesas de votación	c_{tr}: costo de transferir los tokens n: cantidad de mesas $c_{tr} = e * n * p$
Habilitar jornada electoral	c_{hj} : costo de habilitar jornada electoral $c_{hj} = e * p$
Autorización de votos para los electores	c_a : costo total de autorizar tokens n : cantidad total de electores $c_n = e * n * p$
Votación por parte del elector	c_{ve}: costo total de autorizar tokens n : cantidad total de electores $c_{ve} = e * n * p$
Terminar jornada electoral	c_{tj} : costo de terminar la jornada electoral $c_{tj} = e * p$
Costo total de las elecciones	c_{te} : costo total de la jornada electoral en pesos colombianos $c_{te} = c_m + c_t + c_e + c_v + c_{hm} + c_{rm} + c_{tm} + c_{hc} + c_c + c_{tc} + c_{tr} + c_{hj} + c_a + c_{ve} + c_{tj}$

TokenVoteContract tiene un costo en gas de 1.352.345, que en ether es igual a 0,0270469 como se aprecia en la Tabla I, este último valor es el que el minero acredita a su billetera y lo reclamará en una transacción en base a su cotización actual.

Ahora que se tienen los diferentes costos asociados a cada una de las posibles transacciones que se pueden realizar mediante la prueba de concepto, se procede a proponer las diferentes fórmulas para realizar el cálculo del costo de toda una jornada electoral. Para poder calcular los costos de las diferentes transacciones, se puede emplear la Tabla II. Algunas de las variables que no aparecen definidas en la misma son las siguientes:

- p : precio actual del ether.
- e : costo de realizar la transacción que se está evaluando en el momento, en ether.

A partir de la Tabla II, si desea conocer el costo de emitir todos los votos, puede usarse c_{ve}; si se requiere determinar el costo total de todas las transacciones, se puede usar c_{te}. Para poder calcular el tiempo que tardaría la Blockchain en procesar una cierta cantidad de transacciones, subordinada a la cantidad de electores, la cantidad de votos emitidos por las mesas disponibles, y considerando el tiempo promedio de minado de un bloque en la red de Ethereum (aproximadamente 16 segundos), se propone la ecuación: $t = (t_m * e)/n$, en donde:

- t : tiempo empleado para minar la cantidad de votos emitidos.
- n: número de mesas de votación presentes en la consulta.
- t_m: tiempo promedio empleado para minar un bloque.
- e: cantidad de electores potenciales

El escenario relacionado en las Figuras 6 y 7 simula un proceso de votación universitaria, específicamente, una consulta de opinión en la Universidad del Quindío ubicada en Armenia, Colombia; donde en las anteriores elecciones, asistieron 9.897 electores a ejercer su derecho al voto [17], frente a los 13.452 electores (únicamente estudiantes) matriculados en la sede de Armenia de la Universidad [18]. Todos estos electores potenciales debían ser atendidos únicamente por 30 mesas distribuidas dentro de la sede citada [19]. Partiendo de los datos anteriores, se tiene que, cada mesa emitiendo un voto cada 16 segundos aproximadamente, le tomaría a la Blockchain de Ethereum un tiempo aproximado de 1.99 horas procesar dichas transacciones (cantidad de electores anteriormente citados), y 2.5 horas procesar los 17.161 estudiantes activos para el semestre 2018-2 [18] si todos los estudiantes

salieran a las urnas a ejercer su derecho. Estos tiempos se calcularon usando la fórmula definida para la variable t . Así, cuando el encargado de analizar la jornada electoral conozca todos los detalles, se puede inferir que, para 74.250 o más electores, la Blockchain no sería viable para terminar de minar las transacciones en las 11 horas que dura la consulta, pero resultaría viable si en base a los cálculos se extiende el número de horas del proceso electoral.

A. Discusión

Blockchain es una promesa viable para ser usada en contextos electorales pequeños, salvo se extienda el tiempo de duración de la jornada electoral, dado que el minado compromete su rendimiento y escalabilidad. Cabe aclarar, que este tiempo de minado también es su punto fuerte para hacer que los datos almacenados sean seguros, inmutables, y transparentes.

El presente en comparación con otros trabajos como el [6], [7] y [16], propone una forma de voto electrónico similar, evitando ligar la clave pública al voto. Además, se le retira la tarea al votante de guardar el par de claves para poder votar en cada periodo electoral, buscando mitigar los inconvenientes por la pérdida de sus claves. En los trabajos citados en el presente, hay una variedad de propuestas, sin embargo, la forma de implementarlas no es mencionada, y no proveen el software desarrollado, a diferencia del presente.

Esta propuesta no permite la coerción a los votantes, y pueden votar protegidos en los puntos de votación. Caso contrario si votaran desde su casa, sobre todo en zonas hostiles.

B. Implementación en América Latina

Blockchain ha demostrado tener una gran flexibilidad de adaptación, por lo que puede ser implementado en cadenas de suministro, identidad digital, transparencia en procesos de contratación de un gobierno, trazabilidad de productos, transparencia en una ONG, envíos de dinero sin intermediarios o el voto electrónico. Esto puede realizarse a través de una infraestructura propia de una empresa o proveída por un tercero en la nube. Para tener un mejor control sobre las transacciones que se realicen sobre esta tecnología, se hace necesario que cada gobierno expida políticas bien definidas para fines de regulación en la misma.

VI. Conclusiones

El procedimiento del consenso, la ausencia de una autoridad central, sumado a la réplica de información en cada nodo, permite que éstos juzguen inequívocamente si el nuevo bloque a registrar en la Blockchain no altera malintencionadamente la misma, esto promete la inmutabilidad de los votos almacenados, destacando la viabilidad de la tecnología en contextos electorales pequeños. Además, como todo en la Blockchain es público, cualquier persona puede realizar conteo de votos de forma manual y corroborar con los resultados finales, aunque cabe aclarar, que la aplicación no permite el recuento parcial de votos durante la jornada electoral, únicamente cuando se habilita el escrutinio público (en atención al principio de imparcialidad) por parte del Consejo Electoral.

Se hace necesario el trabajar en las identidades descentralizadas para los diferentes electores, por lo que se plantea esto como un trabajo futuro. Donde se encuentre una manera, bajo las restricciones de los principios básicos del voto que se plantearon en anteriores secciones, entregar una identidad digital al elector, sin comprometer su anonimidad.

Para mayor información respecto al trabajo reportado, en https://github.com/BlockchainVotingDemo/sistema-electoral-blockchain, se pone a disposición un video de la prueba de concepto y el código fuente de la aplicación[1].

References

[1] A. A. García, "El voto electrónico en españa," Master's thesis, Universidad Internacional de la Rioja, jul 2016. [Online]. Available: https://reunir.unir.net/handle/123456789/4470

[2] Euskadi, "Voto electrónico. voto electrónico en el mundo," dec 2018. [Online]. Available: https://www.euskadi.eus/informacion/voto-electronico-voto-electronico-en-el-mundo/web01-a2haukon/es

[3] A. Molano, "¿qué es y cómo implementar el voto digital en colombia?" apr 2017, (Accessed on 04/05/2020). [Online]. Available: https://blogs.elespectador.com/actualidad/internet-pal-diario/implementar-voto-digital-colombia

[4] G. Lin and N. Espinoza, "Electronic voting - introduction," 2017. [Online]. Available: https://cs.stanford.edu/people/eroberts/cs181/projects/2006-07/electronic-voting/index.html

[5] N. Saini, H. Verma, and P. Sharma, "An analytical study of e-voting system." *International Journal of Recent Research Aspects*, vol. 4, no. 3, pp. 75 – 85, 2017. [Online]. Available: https://www.ijrra.net/Vol4issue3/IJRRA-04-03-16.pdf

[6] A. Fatrah, S. El Kafhali, A. Haqiq, and K. Salah, "Proof of concept blockchain-based voting system," in *Proceedings of the 4th International Conference on Big Data and Internet of Things*, ser. BDIoT'19. New York, NY, USA: Association for Computing Machinery, 2019. [Online]. Available: https://doi.org/10.1145/3372938.3372969

[7] A. Alam, S. M. Zia Ur Rashid, M. Abdus Salam, and A. Islam, "Towards blockchain-based e-voting system," in *2018 International Conference on Innovations in Science, Engineering and Technology (ICISET)*, 2018, pp. 351–354.

[8] K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri, and S. Gupta, "A comparitive analysis on e-voting system using blockchain," in *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2019, pp. 1–4. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8777471

[9] G. Dagher, P. Marella, M. Milojkovic, and J. Mohler, "Broncovote: Secure voting system using ethereum's blockchain," *ScitePRESS – Science and Technology Publications, Lda.*, pp. 96–107, 2018.

[10] B. Domínguez, "'i-voting', orgullo estonio," mar 2019. [Online]. Available: https://elpais.com/internacional/2019/03/02/actualidad/1551536981_504778.html

[11] G. Lucuy, K. S., and Y. Galaburda, "Modelo y sistema de votación electrónica aplicando la tecnología de cadena de bloques." *RevActaNova*, vol. 9, no. 2, pp. 3–10, jul 2019. [Online]. Available: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1683-07892019000200006

[12] I. Martinovic, L. Kello, and I. Sluganovic, "Blockchains for governmental services: Design principles, applications, and case studies," University of Oxford, Tech. Rep. 7, dec 2017. [Online]. Available: https://www.ctga.ox.ac.uk/sites/default/files/ctga/documents/media/wp7_martinovickellosluganovic.pdf

[13] A. Preukschat, *Blockchain: la revolución industrial de internet*, ser. Sin colección. Grupo Planeta, 2017. [Online]. Available: https://books.google.com.co/books?id=Lb7DDgAAQBAJ

[14] Coinest.co, "¿qué es ethereum network?" Nov 2017, (Accessed on 11/19/2019). [Online]. Available: https://medium.com/@coinest.co/qu%C3%A9-es-ethereum-network-e3fee085709b

[15] Ethereum, "Introducción a los contratos inteligentes," 2017. [Online]. Available: https://solidity-es.readthedocs.io/es/latest/introduction-to-smart-contracts.html

[1] Se recomienda descargar el video y usar un reproductor de video diferente al empleado por el navegador web de forma predeterminada.

[16] N. Kshetri and J. Voas, "Blockchain-enabled e-voting," *IEEE Software*, vol. 35, no. 04, pp. 95–99, jul 2018.
[17] U. del Quindío, "Votación definitiva consulta de opinión para candidatos a rectoría, decanaturas y dirección de programas," Apr 2019. [Online]. Available: https://noticias.uniquindio.edu.co/votacion-definitiva-consulta-de-opinion-para-candidatos-a-rectoria-decanaturas-y-direccion-de-programas/
[18] M. Colombia, "Reporte matriculados por sede 2018-2," Mar 2019. [Online]. Available: https://www.datos.gov.co/educaci-n/matriculados-totales-por-sede-2018-2/fc2w-zrb9
[19] U. del Quindío, "Reporte de votantes consulta de opinión para candidatos a rectoría, decanaturas y dirección de programas," Apr 2019. [Online]. Available: https://noticias.uniquindio.edu.co/reporte-de-votantes-consulta-de-opinion-para-candidatos-a-rectoria-decanaturas-y-direccion-de-programas/

Fáber D. Giraldo System and Computer Engineer from the University of Quindío, Colombia (with a grant from the Ministry of Education of Colombia). He has a Ms.Eng. degree with emphasis on Informatics from EAFIT University, Colombia (with a grant from EAFIT University). He holds a Ph.D. in Informatics from the Universidad Politécnica de Valencia, Spain (with a grant from the National administrative department of Science, Technology and Innovation of Colombia - COLCIENCIAS). He is a full assistant professor in the Faculty of Engineering at the University of Quindío, and also, He is the Head of the Center for Studies and Research in Engineering (CEIFI) of the Universiity of Quindío. His research interests include software engineering, model-driven engineering, software quality, quality in model-driven engineering, software architecture, enterprise architecture and HCI. ORCID: http://orcid.org/0000-0002-6111-3055.

Milton César. Barbosa Systems (Computer) Engineering (1999) with a specialization in Management (2008), a Master degree in Business Administration (2016), and a Ms.Eng. degree in Engineering from the University of Quindío, Colombia (2019). He has 16 years of expertise in working with voting and electoral procedures in the National Registry of Civil Status (Colombia).

Carlos Efrey Gamboa System and Computer Engineer of the University of Quindío, Colombia (2019). He has expertise in the development of web applications,, BlockChain, Smart Contracts, and decentralized apps. His interests are Software Architecture, Artificial Intelligence, Data Sciences, Robotics and Medicine.