|  |  |
| --- | --- |
| FORMATO DE PRESENTACIÓN Y EVALUACIÓN DE ANTEPROYECTO DE TRABAJO DE GRADO  FACULTAD MATEMÁTICAS E INGENIERÍAS |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PROGRAMA | Matemáticas | Ing. Industrial | Ing. de Sistemas | Fecha de entrega | | AÑO | MES | DÍA |
|  |  | x | 2018 | 07 | 13 |
| TÍTULO DEL ANTEPROYECTO: Blockchain y la prevención de fraude electoral | | | | | | | | |
| ESTUDIANTE(S) | | | | | CÓDIGO | | | |
| Camilo Alexander Rodriguez Cuaran | | | | | 506102020 | | | |
|  | | | | |  | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A DILIGENCIAR POR EL COMITÉ DE INVESTIGACIONES** | | | | | | | | | | | |
| **Resultado de la evaluación** | | | | | | | | | | | |
| Aprobado |  | Pendiente de aprobación por correcciones\* | | |  | Reprobado | | | |  | |
| Director asignado: | | | | | | Definitivo | |  | Provisional | |  |
| Correcciones, observaciones, recomendaciones y compromisos\*: | | | | | | | | | | | |
|  | | |  |  | | |  | | | | |
|  | | |  |  | | |  | | | | |
| Nombre y Firma evaluador | | | Nombre y Firma evaluador | Nombre y Firma evaluador | | | Nombre y Firma evaluador | | | | |
|  | | | |  | | | | | | | |
| Director de Programa | | | | Director de investigaciones | | | | | | | |

1. FORMULACIÓN DEL PROBLEMA
   1. Descripción:

En una sociedad democrática los ciudadanos tienen derecho a elegir y controlar a sus gobernantes, así por ello existe un mecanismo de elección el cual cada individuo ejercerá la acción de votar por un representante, allí se hace un conteo de votos y se tienen normas y parámetros para seleccionar el preferido[[1]](#endnote-1); en la mayoría de sociedades democráticas se implementa la elección por mayoreo, en que implica que la persona que obtuvo la mayor cantidad de votos será elegido para representar el pueblo y sus intereses. Pero en las sociedades actuales se implementan demasiadas vías de fraude electoral[[2]](#endnote-2), entre ellas son intercambiar votos por especie, utilizar registros únicos nacionales de difuntos, manipulando las papeletas de votación y en países más modernos, manipulando dispositivos electrónicos o sistemas de software para cambiar los votos, robar e insertar campos en las bases de datos y entre muchos otros mecanismos.

Es allí donde es primordial encontrar otros entes de control y prevención de fraude para estos mecanismos tan importantes en las sociedades democráticas actuales[[3]](#endnote-3). Blockchain es una estructura de datos en que la información contenida se agrupa en grupos (bloques) y que se añade una referencia directa al bloque anterior[[4]](#endnote-4); sin embargo, se requiere que exista una aplicación de por medio capaz de “empaquetar” la información y agregarla a la cadena de bloques existentes, así como también implementar distintos mecanismos de seguridad para prevenir ataques a la información contenida, por lo que se propone implementar un servicio Web (API)[[5]](#endnote-5) de votación electoral que usará una cadena de bloques basada en la propuesta original de Ethereum[[6]](#endnote-6) para generar contratos inteligentes[[7]](#endnote-7) entre pares (el Estado y el votante) para prevenir el fraude electoral, este concepto se denomina “*decentralized autonomous corporations”*[[8]](#endnote-8)[[9]](#endnote-9), finalmente se hará de esta manera para que quedar disponible consumirse en una plataforma web, móvil, SMS y cualquier otro medio electrónico que sea capaz de conectarse a una red de Internet, así mismo se desarrollará una aplicación de interfaz gráfica que demuestre la funcionalidad del servicio.

* 1. Área de conocimiento:

Es indispensable tener conocimientos avanzados de desarrollo de software y un poco de criptografía para entender las nociones básicas de Blockchain, así como también se debe conocer de bases de datos para poder abstraer correctamente las entidades y/o entes en el sistema

* 1. Alcances y delimitaciones:

Se desarrollará un contrato “inteligente” con Solidity[[10]](#endnote-10) para la plataforma de Blockchain en Ethereum para llevar la el conteo de votos en un sistema democrático de votación y así poder elegir un candidato apto. También se desarrollará un servicio web para poder conectarse a Ethereum y poder hacer operaciones por medio de un API y así mismo poder demostrar su uso en un mundo más real, finalmente se desarrollará una aplicación web para conectarse con el API y revisar la funcionalidad propuesta.

1. OBJETIVOS GENERAL

Desarrollar e implementar un servicio web que ejecute una cadena de bloques (Blockchain) para realizar votación por consenso; así como también una aplicación web para implementar el servicio web

1. OBJETIVOS ESPECÍFICOS

* Desarrollar un contrato inteligente en la plataforma Ethereum
* Implementar la cadena de bloques en Ethereum
* Desarrollar un servicio web para conectarse con la plataforma
* Desarrollar una aplicación web para consumir el servicio web

1. MARCO REFERENCIAL[[11]](#footnote-1)

Los sistemas de votación en Colombia se llevan a cabo por medio de papeletas de votación para marcar a los candidatos preferidos, pero esto lleva a que ocurran errores humanos sin intención así como intencionales los cuales promueven el fraude electoral.

1. DISEÑO METODOLÓGICO PRELIMINAR

Para poder solucionar este problema se desea hacer un desarrollo de software en el que consta de varios pasos importantes y definitivos para poder lograr los objetivos.

El primero es desarrollar un contrato “inteligente” en la red de Ethereum y basarlo en ese Blockchain, allí se escoge esta plataforma por su robustez y que así mismo existen múltiples tecnologías que están siendo basadas en esta tecnología, lo cual el objetivo principal de este proyecto es prevenir el fraude electoral y al usar un Blockchain más concurrido la probabilidad de que sea modificado o hackeado es bastante baja. La segunda es desarrollar un servicio web que se comunique con este contrato inteligente y así poder emitir operaciones para que sean expuestas a Internet, buscando que se pueda usar en cualquier plataforma, aplicación y demás. El tercer paso es exponer el servicio a una red, en la que para casos prácticos puede ser en red local (LAN) en caso de ser necesario se podrá poner en un servidor público. Y, por último, el cuarto paso sería desarrollar una aplicación de demostración para consumir el servicio web expuesto y a su vez poder crear registros en el Blockchain de Ethereum y así mismo poder consultar el ganador en las elecciones que se desea prevenir dicho fraude.

1. LISTADO DE ENTREGABLES:

* Código fuente de contrato inteligente
* Código fuente del servicio web
* Código fuente de la aplicación web de muestra
* Website público durante 6 meses para la comprobación del sistema

1. CRONOGRAMA

*Presentar gráficamente en formato Gantt.*

1. BIBLIOGRAFÍA

1. http://web.stanford.edu/~ldiamond/iraq/WhaIsDemocracy012004.htm [↑](#endnote-ref-1)
2. http://www.scielo.org.mx/pdf/rms/v69n1/v69n1a1.pdf [↑](#endnote-ref-2)
3. http://perfilesla.flacso.edu.mx/index.php/perfilesla/article/view/307/260 [↑](#endnote-ref-3)
4. https://poseidon01.ssrn.com/delivery.php?ID=881031104121115078064104029026121088037017063054033022103118072092013119096070070066122030022042108012118124116107067095075092016071069044035003087028092083092109011038062012025001115065105122126113123004007087122116003004107120113125099084004085091096&EXT=pdf [Blockchain Technology: What is it good for?] [↑](#endnote-ref-4)
5. https://www.cs.cmu.edu/afs/cs.cmu.edu/Web/People/NatProg/papers/Ellis2007FactoryUsability.pdf [The Factory Pattern in API Design: A Usability Evaluation] [↑](#endnote-ref-5)
6. https://github.com/ethereum/wiki/wiki/White-Paper [A Next-Generation Smart Contract and Decentralized Application Platform] [↑](#endnote-ref-6)
7. https://arxiv.org/pdf/1703.06322.pdf) [An empirical analysis of smart contracts:

   platforms, applications, and design patterns] [↑](#endnote-ref-7)
8. https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274/ [Bootstrapping A Decentralized Autonomous Corporation: Part I] [↑](#endnote-ref-8)
9. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/ [DAOs, DACs, DAs and More: An Incomplete Terminology Guide] [↑](#endnote-ref-9)
10. https://solidity.readthedocs.io/en/v0.4.24/ [What is Solidity] [↑](#endnote-ref-10)
11. [↑](#footnote-ref-1)