Informe Final de Resultados Prototipo Blockchain

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ MEJOR PARA TODOS

Equipo De Trabajo

Sergio Martínez Medina
Alto Consejero Distrital de TIC
smartinezm@alcaldiabogota.gov.co

Jenny Bibiana Bonilla Ospina
Ingeniera Asesora Alta Consejería Distrital de TIC
jbbonilla@alcaldiabogota.gov.co

Angel Rendón Sánchez
Desarrollador de Software - Universidad Nacional de Colombia - Vivelab Bogotá
amrendonsa@unal.edu.co

Jesus Rodriguez Miranda
Desarrollador de software - Vivelab Bogotá
jrodriguezmi@unal.edu.co

Giorgio Acosta Jaramillo
Maestrante en Diseño - Universidad Nacional de Colombia
Diseñador UX
giacostaj@unal.edu.co

Paola Parra
Diseñadora Gráfica - Universidad Nacional de Colombia
Product Owner del Convenio
ppparram@unal.edu.co

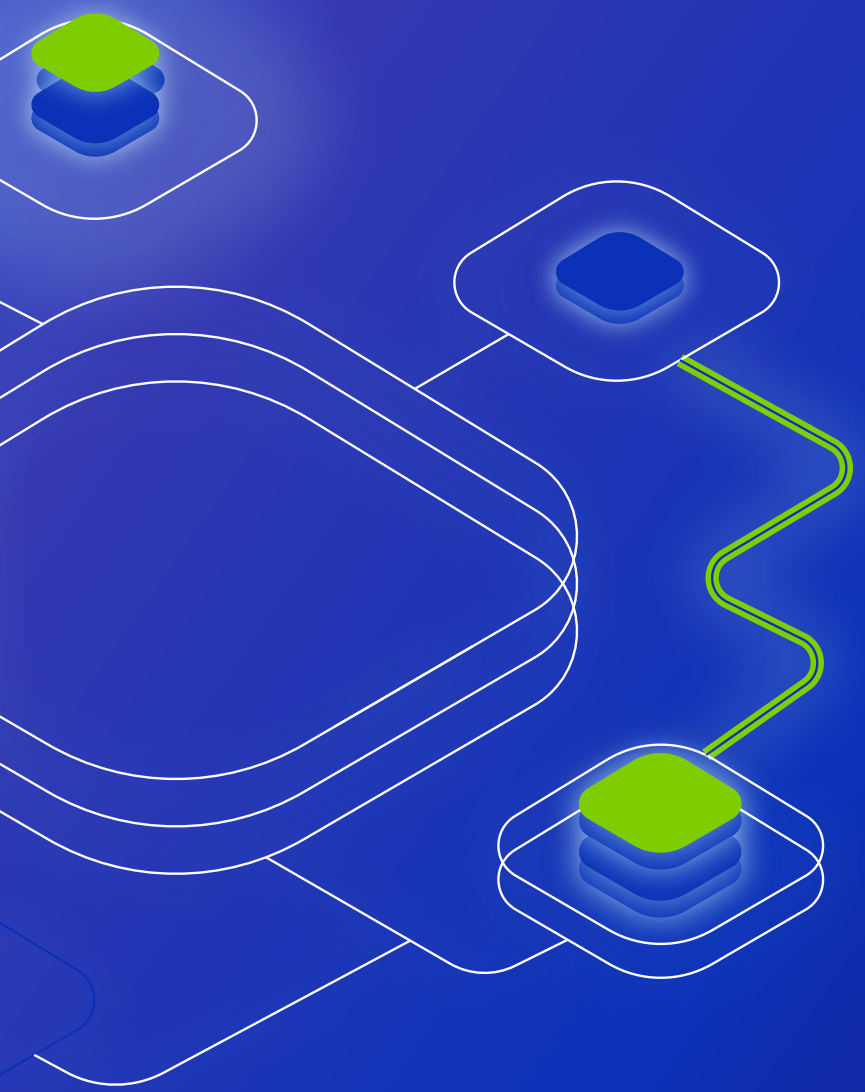


Tabla de Contenido

Tratamiento de Fotos

Para el proceso blockchain llevado a cabo con estudiantes de colegios se registraron evidencias fotografías, estas son de carácter confidencial ya que se considera como información sensible y de carácter restringido en su divulgación, manejo y utilización con terceros.

El registro fotográfico permite sistematizar los resultados del proceso de investigación y trabajo de campo, esta información será usada únicamente con propósitos académicos y de investigación.

Introducción

Bajo la visión del Alcalde Enrique Peñalosa, la tecnología se ha incluido especialmente en el desarrollo de las estrategias educativas, ya que el talento TI se debe empezar a fortalecer desde temprana edad y los estudiantes deben interactuar con los beneficios y el sinnúmero de herramientas que ofrece el mundo digital.

En esta experiencia, fue vital acercar a estudiantes, docentes y a la Secretaría Distrital de Educación, al uso y apropiación de una tecnología compleja como lo es Blockchain, conocida por soportar entre otras, la operación de la moneda Bitcoin, la generación de contratos inteligentes y la capacidad de generar sistemas de elecciones descentralizados. En este sentido, es evidente el objetivo de fortalecer los sistemas educativos públicos, dotándolos de experiencias reales que acerquen a los estudiantes a la tecnología y a la vez, les permita conocer sus múltiples beneficios.

Además de lo anterior, la estrategia Blockchain, fue una iniciativa enfocada en la construcción de justicia, a través de elecciones justas, transparentes, sin intermediarios, que fomentaran la confianza en las instituciones. Asimismo, esta estrategia innovadora buscó modernizar y hacer eficiente los procesos electivos en los colegios públicos de Bogotá, con el objetivo de mostrar a las nuevas generaciones y a los maestros, los beneficios de tecnologías emergentes, para hacer los procesos electorales ágiles, verificables en tiempo real y, confiables en la medida que no necesitan intermediarios.

El presente documento evidencia el resultado del proceso realizado para el desarrollo de un prototipo de elecciones digitales basado en la tecnología Blockchain, en la primera parte se presenta una compilación sobre el estado del arte de esta tecnología a febrero de 2018, así como la importancia de los procesos de gobierno escolar en las Instituciones Educativas Distritales, en la segunda parte se presentan las consideraciones para el diseño del prototipo desde los aspectos técnicos y de contexto del mismo.

En la última parte se describe el proceso realizado en tres instituciones educativas distritales dos de ellas realizaron la elección de sus representantes estudiantiles haciendo uso de la solución propuesta mientras la tercera realizó un proceso pedagógico de reflexión en relación con la importancia de la tecnología para los procesos electorales.

Al final del documento se presenta una serie de conclusiones y recomendaciones sobre el uso de la tecnología Blockchain en procesos de elecciones estudiantiles, los cuales están basados en el prototipo desarrollado para esta experiencia y en el ejercicio desarrollado en los colegios, contemplando los inconvenientes y aciertos presentados durante el experimento.

1 Estado del arte

Cada cierto tiempo, se desarrollan nuevas tecnologías que llegan incluso a impactar la manera como nos relacionamos. Tal fue el caso del internet, que nos permitió acceder a información ilimitada y a una gran cantidad de servicios que buscan mejorar nuestra calidad de vida. También hemos diseñado instituciones que nos ofrecen servicios de acuerdo con nuestras necesidades.

Sin embargo, muchas de esas instituciones carecen de transparencia, acumulan poder, realizan cobros elevados o buscan controlar la información, generando en los usuarios preocupaciones y pérdida de confianza. ¿Son necesarias esas entidades centrales?, o ¿es posible acceder a los mismos servicios con mejor experiencia, de manera segura, transparente y más económica, y además de eso, evitando la centralización? Es decir, que la información no la controle una única parte, sino que la conozcan muchos.

Ese es una gran promesa de Blockchain, pensar un mejor mundo descentralizado, donde la tecnología nos brinda la confianza que históricamente hemos depositado en terceras instituciones, donde muchos de los servicios que ofrecen las instituciones e intermediarios que nos han ayudado hasta hoy, podrán ser mejorados y los usuarios tendremos nuevas alternativas para usar los mismos servicios.

Asimismo, desde el principio la humanidad ha registrado de forma escrita toda suerte de anotaciones con el propósito de controlar y monitorear activos que con mayor frecuencia eran monedas, propiedades y cuentas. Hoy en día esas mismas actividades siguen siendo objeto de nuestro interés, entonces, ¿qué ha cambiado si aún seguimos registrando esos activos? Hemos usado desde tablas de arcilla, pasando por diversos tipos de papel, hasta representaciones binarias en sistemas de cómputo en programas contables (Bauerle, 2017), (Figura 1).

Figura 1. Evolución de los sistemas de registro de activos

Recientemente, nuevas formas algorítmicas permiten la creación colaborativa de registros distribuidos, que no son otra cosa que una base de datos compartida en una red que no conoce límites geográficos, todo individuo participante de esta red, obtiene una copia idéntica de los registros que se encuentran en la misma, y cualquier cambio en su estructura es replicado en cuestión de un par de minutos, e incluso unos cuantos segundos (Grant, 2016).

Los registros adoptan diversas formas que van desde activos financieros, hasta contratos inteligentes, lo que probablemente suscite suspicacias relativas a la seguridad, sin embargo, los registros almacenados se mantienen bajo técnicas criptográficas usando llaves y firmas digitales que controlan quién puede hacer que en la base de datos, dadas unas reglas que todos los participantes aceptan (Grant, 2016).

La Tecnología de Registro Distribuido (DLT por sus siglas en inglés) es el término acuñado para hacer referencia a esa base de datos distribuida. Si bien existen múltiples implementaciones, quizás la

más conocida de todas es la

Blockchain

(cadena de bloques)

como tecnología que soporta la operación de la Bitcoin (*un sistema de dinero digital persona a persona*), dado el impacto que en tiempos recientes ha generado esta criptomoneda por su valorización con respecto a importantes divisas (Lansiti, 2017). Los algoritmos de la Blockchain, permiten que transacciones de Bitcoin se agreguen al registro global (la cadena) como entradas en las páginas de un libro contable (un compendio de transacciones de tamaño fijo, o bloque), ver figura 2, prescindiendo de instituciones terceras, requiriendo únicamente que se solucione el acertijo matemático del algoritmo (Nakamoto, 2008).

Figura 2. Representación de las transacciones en la cadena de bloques

El andamiaje montado por Bitcoin para soportar su operación (la Blockchain), sienta la base para asegurar una gran cantidad de transacciones. Esta aproximación se puede llevar a otros contextos diferentes a los de una moneda criptográfica: firmas digitales, identidad e identificación, registro de propiedades, certificados educativos, emisión de pasaportes, mejora de los servicios de salud, contratos inteligentes y, una gama de posibilidades y herramientas (BTC Studios, 2017).

Los entes gubernamentales tienen en la tecnología Blockchain una herramienta que propende por la transparencia, seguridad y trazabilidad. Al romper con el esquema tradicional de datos centralizados, disminuye los costos de mantenimiento de infraestructura computacional; reduce significativamente el riesgo de ciberataques puesto que la base de datos se distribuye globalmente y todos los participantes pueden detectar anomalías y corregirlas por consenso.

Una muestra de lo expuesto viene tipificada por los esfuerzos de los gobiernos estonio, británico, israelí, neozelandés, y surcoreano, pioneros en la implementación de soluciones basadas en Blockchain, tales como el registro digital de negocios e impuestos electrónicos, disminuyendo la carga administrativa y tributaria (Digital.govt.nz, 2014).

La tecnología BlockChain y las criptomonedas son

de especial interés para los bancos centrales y departamentos financieros gubernamentales por la inherente distribución de valor electrónico y la trazabilidad transaccional de la que carece el papel moneda.

El Decreto 1860 de Agosto 3 de 1994, por el cual se reglamenta parcialmente la Ley 115 de 1994, en los aspectos pedagógicos y organizativos generales en sus artículos 28 y 29, brinda el marco para desarrollar tal prototipo en cuanto la elección del Personero de los Estudiantes se configura como un mecanismo de fortalecimiento y participación con el que se pretende enseñar a los estudiantes la importancia de la democracia y sus pasos. Siendo así la elección del Personero de los Estudiantes la oportunidad de probar dicho prototipo en un ambiente real, evidenciando, no sólo las bondades ya expuestas, sino transmitiendo el mensaje de gobernabilidad incluyente, transparente y trazable a los jóvenes y niños que participen de este proyecto (Ley N°115, 1994).

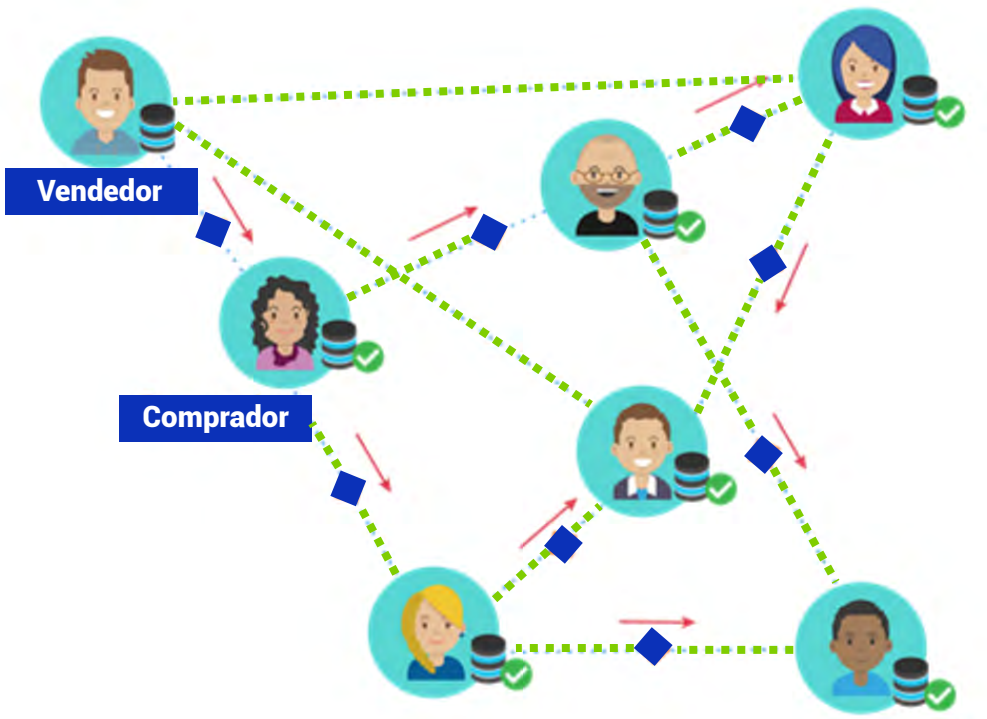
En el marco del convenio entre la Alcaldía de Bogotá y el Vivelab de la Universidad Nacional, se propone un experimento a través del desarrollo de un prototipo de votaciones electrónicas para elecciones de representantes estudiantiles, que aseguren la información en la Blockchain, para brindar transparencia, confianza, trazabilidad, e inmutabilidad en los procesos electorales.

1.1
¿Qué es la tecnología Blockchain?

Para explicar qué es Blockchain, es necesario aclarar qué es la Tecnología de Registros Distribuidos (Distributed Ledger Technology), o DLT por sus siglas en inglés. Una DLT es "un tipo de base de datos que se comparte, replica y sincroniza entre los miembros de una red" (Brakeville, 2017), la DLT registra toda transacción de los participantes en la red (Figura 3).

La dinámica de participación se acuerda por consenso entre todos los participantes de la red, eliminando todo intermediario del proceso. El consenso es un protocolo que todos los participantes conciertan cumplir y que confía en el poder criptográfico de las funciones hash2 y las firmas digitales o firmas criptográficas3, este protocolo asegura que existen miles de copias de la cadena de bloques distribuidas globalmente, donde el riesgo disminuye, ya que un fraude debe ocurrir simultáneamente en muchos nodos de la red en exactamente el mismo momento. "Todo registro en la DLT tiene una estampa temporal4 y una firma criptográfica"(Brakeville, 2017), permitiendo que el sistema sea auditable, (Figura 4).

Figura 3. Distribución de datos a través de una red descentralizada



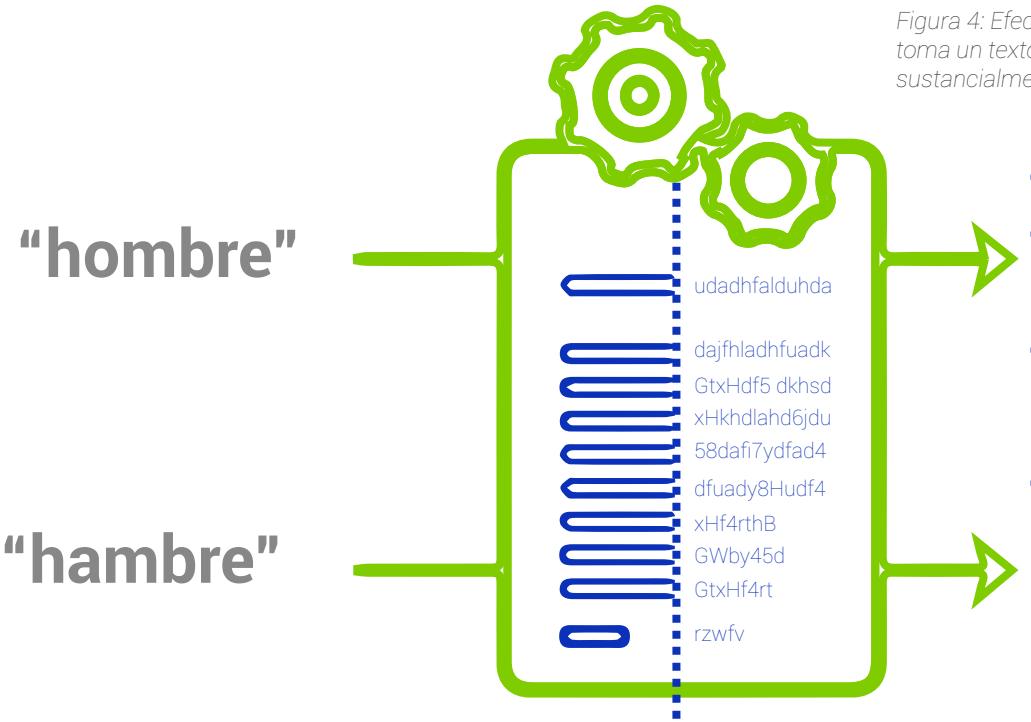


Figura 4: Efectos de la función hash sha256 en dos textos diferentes. La función hash sha256 toma un texto y calcula uno nuevo, si el texto cambia así sea por una sola letra, el resultado es sustancialmente diferente. Imagen propia.

La Blockchain, es en sí una forma de DLT, que registra permanentemente transacciones en forma de bloques tipo hash que se enlazan en una cadena criptográfica secuencial con duplicados en miles de computadoras alrededor del mundo, en redes persona a persona (peer-to-peer) públicas o privadas. Es evidente de dónde viene el nombre: una cadena de bloques que no puede ser alterada retrospectivamente (Brakeville, 2017).

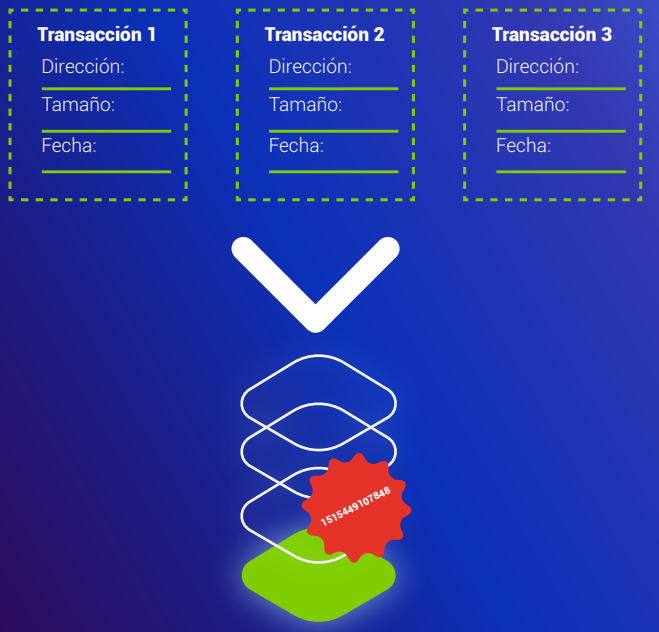
Para entender cómo funciona una red Blockchain, se propone como ejemplo la misma dinámica que se quiere abordar: la elección del Personero de los Estudiantes en los colegios. Para un colegio determinado hay un grupo de candidatos. Cada estudiante del colegio debe registrar su voto por el candidato de su predilección. Cuando un estudiante marca su voto, este se registra como una transacción, y con una estampa temporal (Figura 5). Finalmente se comparte con otros computadores en la red de Blockchain.

Figura 5: Panel de selección de candidatos

A medida que más y más votos se registran, se generan nuevas transacciones. Esas transacciones se combinan entre sí, cuando se combinan suficientes transacciones se empaquetan en un bloque de tamaño fijo. Una vez que un bloque se completa se le imprime su estampa temporal. (Figura 6)

El bloque se envía a la red de Blockchain, donde se revisa su estampa temporal y decide dónde se ubica: justo después del último bloque que se agregó previamente. Así, bloque tras bloque se va formando una cadena. De aquí viene el nombre de la tecnología: una cadena de bloques.

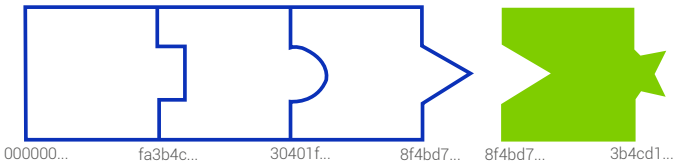
Figura 6: Transacciones, cadena de bloques y estampa temporal



Para unir bloques, como si se tratase de una especie de cemento, se usa nuevamente una función hash sobre el bloque anterior, generando un texto único, que resulta ser una especie de eslabón de la cadena: el texto generado se incluye en el nuevo bloque lo que enlaza a ambos y permite que se trace la información coherentemente. El proceso se repite tantas veces como bloques nuevos vayan llegando a la red.

Antes de permitir que un bloque se añada a la cadena, hay un proceso de verificación que analiza el resultado de la función hash aplicada al bloque anterior: el mecanismo detecta cualquier anomalía en ese bloque y su efecto en el actual, impidiendo que el encadenamiento suceda..

Figura 7: Representación del proceso de verificación de los bloques



Mientras los bloques se agregan a la cadena, de forma paralela la nueva configuración adoptada por ésta se redistribuye entre todos los nodos de la red. Así cada participante de la red obtiene la información más reciente de estas operaciones. El procedimiento recién explicado es el que garantiza que la información registrada en la cadena de bloques sea casi imposible de modificar.

Este flujo se basa en cinco principios subyacentes de la tecnología (Iansiti, 2017), los cuales se describen a continuación:

1. **La base de datos se debe distribuir.** Cada nodo en la red tiene acceso a toda la base de datos. No hay participante que tenga más privilegios que otro. Todos los participantes pueden auditar y controlar la información (Brakeville, 2017).

2. **La transmisión y distribución ocurre directamente entre pares.** No hay un nodo central por el que la base de datos se replique. El modelo exige que tal actividad ocurra entre nodos (Iansiti, 2017).

3. **Transparencia con o sin privacidad.** Toda transacción ocurre entre direcciones de la cadena de bloques. Los nodos, o usuarios, en la cadena se identifican por medio de un texto alfanumérico de treinta o más caracteres. Los usuarios pueden decidir si revelan su identidad mediante prueba o no (Iansiti, 2017).

4. **Inmutabilidad de registros.** Quizás una de las características más importantes de esta tecnología. Una vez que una transacción se encadena, ésta no puede ser alterada porque se enlaza a todo registro transaccional previo y futuro (Iansiti, 2017). Bajo el supuesto de que se pudiera hacer, la cadena se rompe.

5. **Lógica computacional.** Las transacciones entre direcciones están atadas inherentemente a lógica computacional, lo que se traduce en que los usuarios pueden configurar algoritmos y reglas que disparan transacciones entre nodos (Iansiti, 2017). Esta característica abre la posibilidad de usar la tecnología Blockchain para transar, no únicamente valor por algún tipo de moneda criptográfica, sino cualquier otro tipo de activo (como los contratos inteligentes).

1.2
Ventajas de la tecnología Blockchain

Los beneficios implícitos dada la topología dispuesta por una red de cadena de bloques, e incluso otras formas de DLT, se pueden resumir en los siguientes seis grupos:

Eficiencia.
Hay una reducción considerable en términos de tiempo y costos. Estas reducciones son producto de la forma en la que opera la red: las transacciones se dan entre pares y se elimina de todo proceso a un intermediario (Brakeville, 2017).
Esto permite que se lleven dinámicas analógicas a contextos digitales. En los procesos electorales se reducen los costos asociados a la elaboración y distribución de tarjetas electorales, así como costos implícitos en la logística para estos procesos. El tiempo de conteo queda incluido en el mismo proceso electoral: cuando se registra un voto, este se registra en el contador del candidato elegido.

Auditoría.
Aparte de reducir los costos y el tiempo en los contextos regulatorio y control, los mecanismos de inmutabilidad de la Blockchain, ofrecen la posibilidad de permitir el análisis de cómo se dieron las transacciones, ya que queda un rastro generado por las funciones hash (Treagust, 2017). Nadie puede atribuirse la total pertenencia de la información, como tampoco atribuirse la autoría original de toda la información, es un sistema donde las transacciones son producto de las operaciones de todos los participantes, lo que "incrementa la confianza e integridad en el flujo de información transaccional entre miembros participantes" (Brakeville, 2017). Asimismo, permite que en cualquier momento se pueda iniciar un proceso de auditoría sobre un proceso electoral determinado, analizando no solamente si el total de los votos registrados corresponde al número de sufragantes, sino que permite corroborar identidades manteniendo el voto secreto, protegiendo al sufragante.

Trazabilidad.
Quizás el ejemplo más contundente es la adopción de la Blockchain en la industria de piedras preciosas, donde la tecnología de cadena de bloques permite la traza de diamantes desde la mina hasta el usuario final (Iansiti, 2017).

Transparencia.
Una información consistente con reducción de errores, resultado de los mecanismos de consenso, ofrece el detalle de cada transacción y los participantes envueltos en ella (Brakeville, 2017). En los procesos electorales, esto consolida la construcción de confianza ciudadana basada en transparencia y no en reputación.

Seguridad.
Gracias a los complejos procedimientos criptográficos, es posible garantizar la autenticidad de la información (Treagust, 2017). La generación de nueva información es el producto de una línea coherente de bloques previos combinando las transacciones nuevas, cualquier intento de añadir transacciones nuevas sin conocer la información de los bloques previos, evita que información corrupta se agregue al bloque. La inmutabilidad de los bloques también brinda la salvaguarda de los datos allí contenidos. Para procesos electorales estas dos características de seguridad crean el ambiente propicio para que se aseguren las actividades de elección y consulta.
Retroalimentación. La información generada resultante de las dinámicas electorales y

permite el mejoramiento del código informático para incluir características que enriquezcan la información.

1.3
Usos y aplicaciones

La tecnología Blockchain al tener la capacidad de generar intercambio de valor e información de una forma segura, se puede usar para una variedad de industrias, permitiendo transferencias de datos más eficientes entre entidades. Es posible visualizar su uso en muchas áreas, tales como:

En el sector financiero.
En la actualidad las transacciones financieras internacionales se deben realizar en horarios de oficina, en algunos casos pueden tomar hasta varios días en ser aprobadas. En una plataforma financiera basada en Blockchain, las transacciones son procesadas a cualquier hora, y el tiempo en ser verificadas y completadas puede ser en minutos. El ejemplo más exitoso es el mismo Bitcoin, que se ha convertido en un activo digital que se ha extendido en todo el mundo.

Para guardar y crear contratos inteligentes (smart contracts).
La ventaja de la tecnología Blockchain se basa en la confianza, por lo que se podrían desarrollar contratos inteligentes "los smart contracts son aplicaciones que se ejecutan exactamente como se programaron sin posibilidad de tiempo de inactividad, censura, fraude o interferencia de terceros" (Ethereum, 2017), en el que si se cumple una condición (verificable por un sistema informático) se realiza una cierta operación, sin intervención de un tercero.

Para realizar el seguimiento de productos y servicios.
Se puede realizar una trazabilidad para mantener un registro del origen de un producto y saber así su procedencia, a través de un identificador único. El sistema garantizará en todo momento la privacidad de la información trazada, por ejemplo realizar un seguimiento de cada una de las piezas que componen un móvil, tableta, TV, coche o incluso obras y proyectos.

Para validación de derechos de autor.
Para garantizar a los artistas y coleccionistas un registro digital de sus obras, se puede guardar sobre un bloque de Blockchain, un identificador único con información de una obra, que permita llevar su control y seguimiento. Esto se podría usar con películas, música, etc., lo que podría permitir remunerar al autor por el uso que se hace de su obra automáticamente.

En la salud.
Puede usarse Blockchain, para guardar la información de historiales médicos y así mantener su privacidad, así la información de un usuario no podría ser modificada garantizando la validez de los datos.

Para identificación de usuarios.
Para crear sistemas de identificación, donde cada usuario pueda tener un token de reconocimiento único, confiable, universal e inmutable para cada usuario, que permitiría el acceso a sistemas seguros, garantizando, por ejemplo, que una entrada a un concierto o evento sea original.

En los servicios de notaría y legales.
El intermediario, como entidad que vigila que se cumpla la ley, puede ser eliminado de la transacción, si los procesos legales se completan siguiendo los parámetros programados en el contrato inteligente, por ejemplo, los beneficiarios de un testamento, que se ejecuta y distribuye sin intervención de un notario.

En seguridad y defensa.
El acceso no autorizado a una infraestructura de defensa de vital importancia, como puede ser un firmware de red o sistema operativo, puede llevar a que la seguridad nacional se vea seriamente comprometida. Los sistemas

informáticos e infraestructura de defensa se suelen distribuir en diferentes localizaciones, si esta distribución se basara en tecnología Blockchain se aseguraría que el acceso dependa de un consenso, a la hora de modificar información de equipos y redes. Ejemplo, para cambiar la información de una infraestructura de defensa que no se haga en un solo punto de la red, sino que haya consenso entre varios puntos para realizar modificaciones o accesos autorizados.

Para los procesos electorales.
La tecnología Blockchain proporciona una plataforma descentralizada, que permite a los usuarios transferir información de forma segura. Llevando estas características hacia un proceso de votación, los participantes pueden saber que sus votos no serán alterados, su identidad no estará en riesgo y que el conteo de votos será absolutamente transparente. Esto quiere decir, que se podría alcanzar una elección 100% democrática.

Con un sistema electoral y de votación basado en Blockchain, el árbitro electoral es la misma plataforma, ya que los resultados, además de ser registrados en tiempo real, serían inmutables por lo tanto inmodificables y estarían a la vista de los ciudadanos hasta el final del proceso. Para comprender, la tecnología Blockchain es una base de datos distribuida o (Distributed Ledger Technology DLT) "pública o privada" (Vitalik, 2017), que establece consenso para la toma de decisiones sobre la red, y es compuesta por una cadena de bloques en la cual se guardan los datos, por lo tanto una vez que un dato ha sido escrito en un nuevo bloque, con un sellado de tiempo (Time Stamp) y con un enlace al bloque anterior, no puede modificarse. Por esta razón, se puede usar para almacenar de forma creciente datos ordenados en el tiempo y sin posibilidad de modificación ni revisión a menos que sea un Blockchain editable, en cuyo caso, de igual forma deja un registro de la modificación. Las bases de datos distribuidas garantizan que todas las partes vean la misma información, sin que una parte tenga que confiar en que la otra sea honesta, ya que los datos escritos en los bloques, no se pueden falsificar o alterar una vez que estén registrados en la Blockchain. Así que, aplicado a un sistema de votación, hace muy difícil el fraude por modificación de datos, pues supondría atacar al menos el 51% (la mayoría) de los nodos a la vez para tratar de alterar un resultado. Existen dos plataformas que trabajan bajo estos conceptos, tales como:
Democracy Earth (https://www.democracy.earth/) y Follow My Vote (https://followmyvote.com/), que han vuelto realidad estas premisas sobre redes blockchain.

1.4
Referentes nacionales

En los últimos años son varias las iniciativas a nivel nacional que buscan explotar el potencial de esta tecnología, tales como:

- **Vivelab Bogotá.** Ha sido pionero en la propagación sobre el interés y estudio de Blockchain. Junto al Ministerio TIC y Colciencias, realizó la primera Hackatón sobre el tema en Colombia, con la participación de más de 60 desarrolladores, así como, un pabellón exclusivo durante dos días en Colombia 4.0 con charlas y conferencias con expertos en el tema.
- **Plebiscito digital.** Una iniciativa para permitir a los expatriados participar en el plebiscito por la paz de 2016, basada en Blockchain. La OCDE reflejó este proceso,

comentando el impacto y el futuro de Blockchain en los procesos electorales (OCDE, 2016).

- **Buda.com.** Es una empresa chilena con sede en Colombia que desarrolla y opera servicios utilizando la tecnología Blockchain para el sector financiero permitiendo intercambio de criptodivisas para Colombia.

- **Banco de la República.** El Banco de la República Colombia, formalizó un convenio con la compañía de software empresarial R3, que le permite conocer y experimentar los últimos avances en la tecnología de registros compartidos (Distributed Ledger Technology) que se basa en la tecnología Blockchain.

- **Bancolombia y Carvajal.** Diseñaron una plataforma de facturación electrónica que gestiona y almacena de forma encriptada la información de las facturas en Blockchain (Semana, 2017).

1.5
Referentes internacionales

Son varias las iniciativas a nivel internacional que buscan explotar el potencial de esta tecnología:

- **Bitcoin.** Es la aplicación original publicada en el white paper5 escrito por Satoshi Nakamoto en el 2008, donde explica los aspectos principales de la tecnología Blockchain. Es una red P2P (Peer to peer) o entre pares para crear, gestionar y transferir bitcoins de forma colectiva por la red.

- **Ethereum Foundation.** Tiene como misión promover y soportar la plataforma Ethereum y su capa de investigación, desarrollo y educación para enlazar protocolos y herramientas descentralizadas que permitan a los desarrolladores producir la próxima generación de aplicaciones descentralizadas (dapps) y construir una red Internet más accesible, libre y confiable.

- **Hyperledger.** Es un proyecto colaborativo de código abierto que cruza diversas industrias y servicios para el desarrollo de una plataforma basada en Blockchain para aplicaciones transaccionales que permita confianza, responsabilidad y transparencia.

- **R3.** Es una empresa apoyada por instituciones financieras que desarrolla la plataforma Corda para aprovechar el potencial de DLT (Distributed Ledger Technology) para el uso de servicios financieros.

- **Aragon.** Es una aplicación para enlazar la transparencia y el gobierno independiente de cualquier organización, a través de la tecnología Blockchain que permite cambiar los incentivos que tiene la gente para interactuar con otra.

- **IBM.** La capa de negocio que permite crear aplicaciones sobre Blockchain a través de Bluemix, se ha convertido en un espacio de investigación y desarrollo que permite desarrollar con muchas herramientas a disposición, aplicaciones sobre Blockchain.

1.6
Contratos inteligentes

Uno de los usos más significativos que se pueden realizar sobre las Blockchain públicas, es la idea de implementar smart contracts (contratos inteligentes), mientras un contrato tradicional define los términos de una relación entre dos partes (casi siempre en términos legales) en un documento en papel, el contrato inteligente define esa relación a través de un código criptográfico (Figura 8).

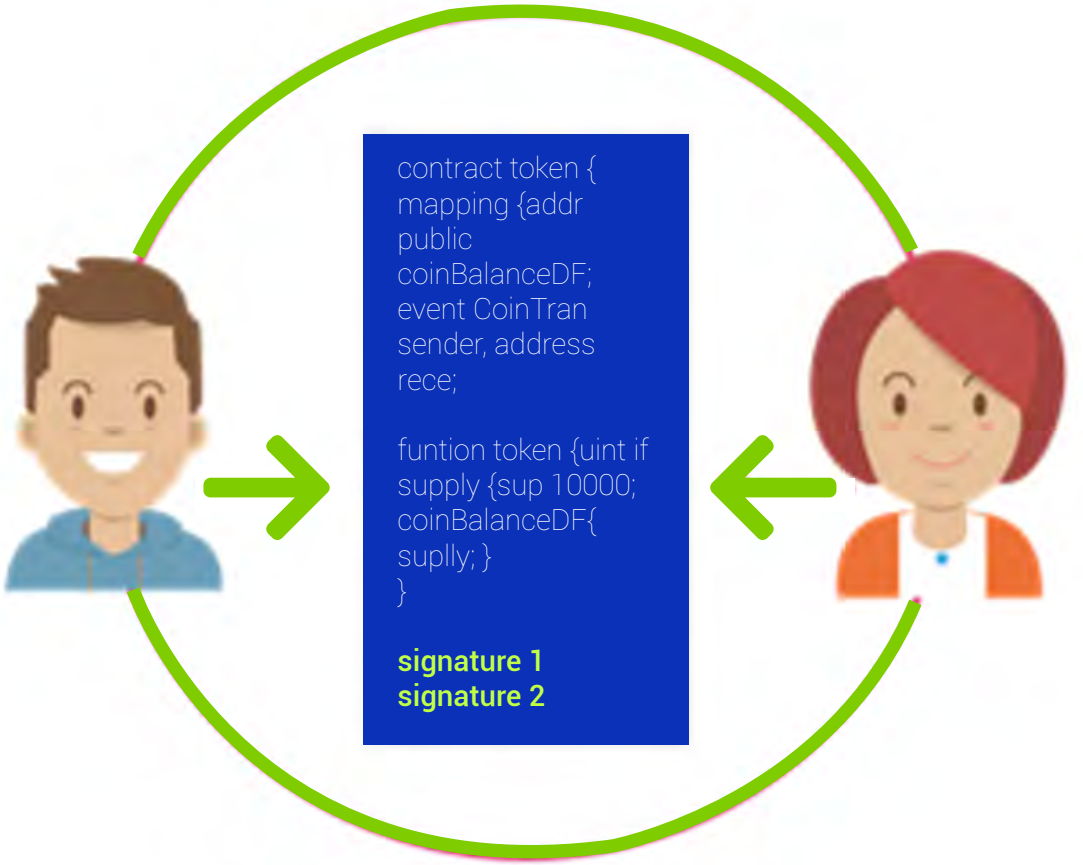


Figura 8: Representación del contrato inteligente entre las partes mediante código

Este concepto fue ideado en 1996 por el célebre jurista y científico de la computación Nick Szabo, en su artículo llamado Smart Contracts: Building Blocks for Digital Free Markets (Szabo, 1996) y luego retomado en Formalizing and Securing Relationships on Public Networks (Szabo, 1997), en el que detalla cómo las personas introducen un dato digital a una máquina y reciben un producto real, sin intermediación de un tercero (Ridley, 2017).

Un ejemplo puede ser un empresario que necesita enviarle suministros de ropa deportiva a un cliente cada cierto tiempo, se programa un código que envíe primero la solicitud de pago, luego de confirmar el recibido del mismo, enviar una notificación al departamento de producción para remitir el pedido, y al ser despachado notificarle al cliente. Este contrato se guarda en la red pública de Blockchain disponible para guardar estos programas, para que no se cambien las condiciones, ni se modifiquen sus funciones y pueda ser ejecutado.

Ethereum es una plataforma creada específicamente para crear contratos inteligentes, también existe una iniciativa conocida como RSK para guardar estos contratos en la red pública de Blockchain de Bitcoin, así como la plataforma Hyperledger que usa su propia red de Blockchain, y otras como Particlm pero enfocándonos en Ethereum, la definición de contrato inteligente según la Ethereum Foundation (2016), afirma que:

"Un contrato inteligente es una colección de código (sus funciones) y datos (su estado) que reside en una dirección específica en la Blockchain de Ethereum. Las cuentas de contrato pueden pasar mensajes entre ellos, así como también realizar cálculos completos de Turing. Los contratos se almacenan en la cadena de bloques en un formato binario específico de Ethereum llamado Ethereum Virtual Machine (EVM) bytecode. Los contratos generalmente se escriben en un lenguaje de alto nivel como Solidity y luego se compilan en bytecode para ser cargados en la Blockchain de Ethereum. (p. 1)"

Siguiendo esta idea, la red Ethereum da la posibilidad a los desarrolladores de programar autonomous agents (agentes autónomos) que "viven" dentro del ambiente de ejecución de Ethereum, siempre computando la pieza específica de código, cuando es "pulsado" por un mensaje o transacción, y teniendo control inmediato sobre su propio equilibrio de éter y de datos. (Vitalik, 2013).

Este concepto que ha evolucionado desde los tiempos de Szabo, se ha convertido en parte fundamental del crecimiento de la tecnología Blockchain en los últimos tiempos y se considera como la parte más prometedora. El parlamentario Lord Holmes of Richmond considera que la Gran Bretaña debe estudiar profundamente cómo esta tecnología puede revolucionar el trabajo del gobierno. (Ridley, 2017).

Cabe anotar que un contrato inteligente es un programa o software, y puede tener los vicios del programador. De todas formas, si se desarrolla con los más altos estándares de la industria, están para quedarse.

Características de un contrato inteligente

Autonomía. Las partes hacen el acuerdo, sin necesidad de intermediarios para confirmar la ejecución, por lo tanto, se suprime el peligro de manipulación por parte de un tercero, ya que el contrato es manejado automáticamente, en lugar de por uno o más individuos, posiblemente parciales que pueden equivocarse.
Confianza. los contratos se guardan en el libro compartido (distributed ledger) de Blockchain. El cual es inmutable y no se puede editar después de haber sido escrito.

Copia de seguridad. sobre Blockchain, la información que guardemos se replica en todos los nodos de la red, por lo tanto, hace casi imposible la pérdida de información.
Seguridad. La información sobre la Blockchain no puede ser cambiada, sin tener al menos el 51% de los nodos en consenso para ese ajuste o cambio, por lo tanto, se puede garantizar que un contrato inteligente que se ejecuta sobre una red pública de Blockchain no puede ser hackeado.

Velocidad. El gasto de tiempo y papeleo para procesar manualmente un contrato, puede ser muy alto. Con el uso de tareas automáticas a través de contratos inteligentes, se pueden salvar muchas horas de trabajo.

- **Ahorro.** Al evitar el uso de intermediarios esto ahorra los costos de intermediación que en algunos casos pueden ser muy altos.
- **Exactitud.** Los contratos no son solo rápidos y baratos, sino también se puede garantizar la exactitud sin errores de las operaciones ejecutadas, si el programa fue bien desarrollado.

A continuación, se presenta una lista de las redes públicas de Blockchain que soportan contratos inteligentes:

- **Ethereum.** Es la red más utilizada en la actualidad y en donde se ejecutan la mayor cantidad de contratos inteligentes.
- **Bitcoin.** Aunque tiene limitada capacidad para guardar documentos, se han realizado algunos ajustes por compañías como RSK, para habilitar su uso sobre bitcoin.
- **Qtum.** Es un esfuerzo de conjugar las dos redes, Ethereum y Bitcoin, para el uso de contratos inteligentes.
- **NXT.** Es una red pública de Blockchain que pone a disposición una serie de plantillas de contratos inteligentes.
- **Particl.** Es una compañía de comercio

electrónico sobre Blockchain que hace uso de contratos inteligentes sobre la red Bitcoin.

1.7
Gobierno escolar

El Ministerio de Educación Nacional de Colombia define al Gobierno Escolar como una forma de preparación para la convivencia democrática, por medio de la participación de todos los estamentos de la comunidad educativa en la organización y funcionamiento del Proyecto Educativo Institucional (PEI).

El Gobierno Escolar está integrado por el Consejo Directivo, el Rector, el Consejo Académico, las comisiones de Evaluación y Promoción, el Personero Estudiantil, el Consejo Estudiantil, el Comité de Bienestar Institucional, el Consejo Disciplinario, el Consejo de Profesores, la Asociación de Padres de Familia y el Comité de Admisiones. Cada uno de los anteriores estamentos promueven los valores que identifican al colegio y velan por el cumplimiento de las normas establecidas en el Manual de Convivencia.

En la actualidad, son los personeros estudiantiles quienes están liderando actividades propias de su labor, pues cierto espacios les exigen de alguna forma que sus propuestas se ejecuten tal y como lo planearon en sus respectivas campañas y además, sean puestas en común.

1.7.1
Aventura democrática

El gobierno estudiantil es un espacio real de formación para la democracia, que se evidencia en la posibilidad de los estudiantes para elegir y ser elegidos, representar los intereses de su comunidad y desarrollar su capacidad de liderazgo político en la institución y su entorno local.

El Gobierno Escolar es una estrategia curricular que promueve el desarrollo afectivo, social y moral de los estudiantes a través de actividades vivenciales. Es una organización de los estudiantes y para los estudiantes que garantiza su participación activa y democrática en la vida escolar; los estimula a participar; los impulsa a actuar en actividades en beneficio de la escuela y la comunidad; les informa comportamientos cívicos y democráticos y actitudes positivas hacia la convivencia, la tolerancia, la solidaridad, la cooperación, la ayuda mutua; los capacita para la toma de decisiones responsables, el trabajo cooperativo, la gestión y liderazgo, la autonomía; los forma para el cumplimiento de sus deberes y el ejercicio de sus derechos.

Desde el aula el niño se acostumbra a participar en distintas actividades tales como: manejo y cuidado de la higiene y la salud, promoción de campañas ecológicas, mejoramiento académico, organización de las áreas de trabajo dentro y fuera del aula, actos culturales, recreativos, religiosos, etc.

Los estudiantes organizan el gobierno democráticamente y forman comités y con la orientación del maestro, preparan sencillos proyectos y los ponen en marcha. El gobierno estudiantil también toma en cuenta la participación de los padres de familia en muchas de estas actividades. (Ministerio de Educación Nacional de Colombia, 2010)

2. Prototipo

2.1

Diseño conceptual

A continuación, se muestran los parámetros de diseño contemplados para el prototipo Blockchain, desarrollo de wireframes en formato de papel, así como su versión digital.

2.1.1

Wireframes

En este apartado se presenta un acercamiento al esquema de la plataforma muy cercano al diseño definitivo.

2.1.1.1.

Página de identificación

Figura 9 Wireframe realizado con la herramienta online Wireframe.cc

2.1.1.2.

Página para votación

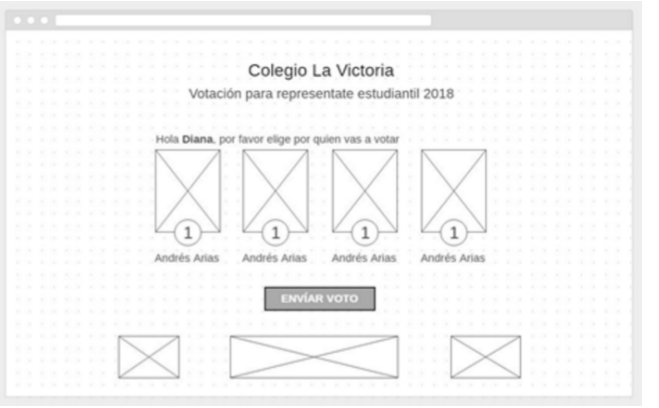


Figura 10 Wireframe realizado con la herramienta online Wireframe.cc

2.1.1.3.

Página de votación exitosa

Figura 11 Wireframe realizado con la herramienta online Wireframe.cc

2.1.2

Parámetros de diseño

A continuación se muestran los parámetros de diseño contemplados para la plataforma de votación estudiantil.

2.1.2.1

Paleta de colores

Se hará uso de una paleta de colores que tengan afinidad con aspectos futuristas, colores brillantes y oscuros, que tenga un aspecto moderno y elegante a la vez. Entendiendo que los usuarios de este prototipo serán niños y jóvenes con un rango de edad entre los 5 y 18 años.

Principal	Secundario	Complementario
#00436c	#194419	#4c0a0a
#71e2df	#42e26b	#ce2929
#a1fbff	#67c674	#ff6666
#cffaff	#9df4ab	#ff8585
#19ade4	#c8fcce	#ffc5c5
#595959		
#95989a		
#e2e2e2		

2.1.2.2
Tipografía

Se hará uso de la familia tipográfica Roboto para el cuerpo de la página, especialmente diseñada para legibilidad en pantallas, y Bree Serif para el título del colegio.

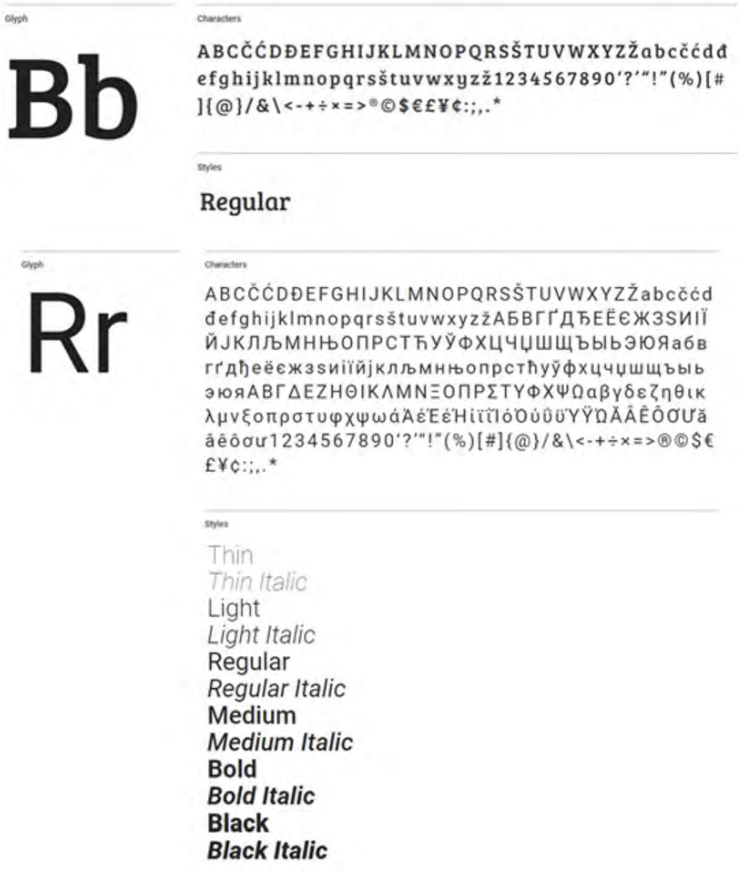


Figura 12 Tipografía del prototipo

2.1.2.3
Iconos

Con el propósito de mantener la esencia de lo moderno, se busca de igual manera un estilo que vaya dirigido a una audiencia de jóvenes. A continuación se presenta una serie de ejemplos de los iconos que se usarán dentro de la plataforma.

a Icono de ayuda

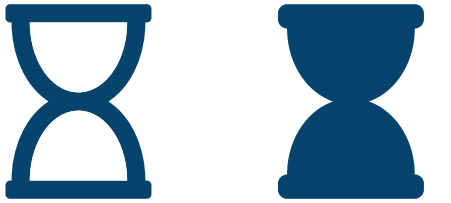
Los iconos de ayuda servirán como accionables de pop-ups en caso de que los estudiantes tengan dudas de algún procedimiento.

b Icono de éxito o votación satisfactoria

El estudiante al realizar el envío del voto, podrá apreciar un icono relacionado a éxito en el proceso.

c Icono de espera o cargando

La plataforma deberá tener un elemento de retroalimentación en caso de que haya una demora, ya sea en el proceso de identificación o de votación, por lo tanto, habrá un icono de carga que estará en movimiento.



2.1.2.4
Elementos interactivos

De acuerdo con los colores y la tipografía elegida, se diseñaron los principales elementos de interacción que irían dentro de la plataforma.

a Botones

Habrá dos estados en los botones; un botón con estado de habilitado, es decir que podrá ser accionado, y otro en estado de deshabilitado que aparecerá hasta que el usuario cumpla una serie de requerimientos, como por ejemplo en caso de que la caja de identificación esté vacía o en caso de que no se haya seleccionado un candidato en la página de votación.

Botón deshabilidato

ENTRAR A VOTAR

b **Desplegable**

Este componente contendrá los colegios disponibles para ejecutar las votaciones.

Colegio Unión Colombia

c **Mensaje popup**

Este componente contendrá los colegios disponibles para ejecutar las votaciones.

El código de estudiante No. **AM110111** no se encuentra habilitado para votar.

VOLVER

2.1.3
Diseño en digital

A continuación se muestran las principales páginas de la plataforma, el orden sería de acuerdo al flujo de votación que el estudiante se encontraría al realizar la actividad misma.

2.1.3.1
Página de identificación

El estudiante deberá escribir su número de identificación de acuerdo al tipo de la misma, cuando la caja de texto esté vacía, el botón de ENTRAR A VOTAR estará deshabilitado.

Figura 13 Diseño propio

2.1.3.2
Página de votación

En la página de votación, el estudiante verá su nombre y se le pedirá que seleccione un candidato por quién votar, al igual que en la página de identificación, el botón estará deshabilitado hasta que no se haya seleccionado un candidato por cada cargo. Al hacer clic se mostrará un mensaje de confirmación antes de poder enviar el voto.

Figura 14 Diseño propio

2.1.3.3

Página de votación exitosa

Una vez que el sistema registre el voto, se podrá ver un mensaje de satisfacción en el proceso, y al estudiante se le entregará un número de verificación.

Figura 15 Diseño propio

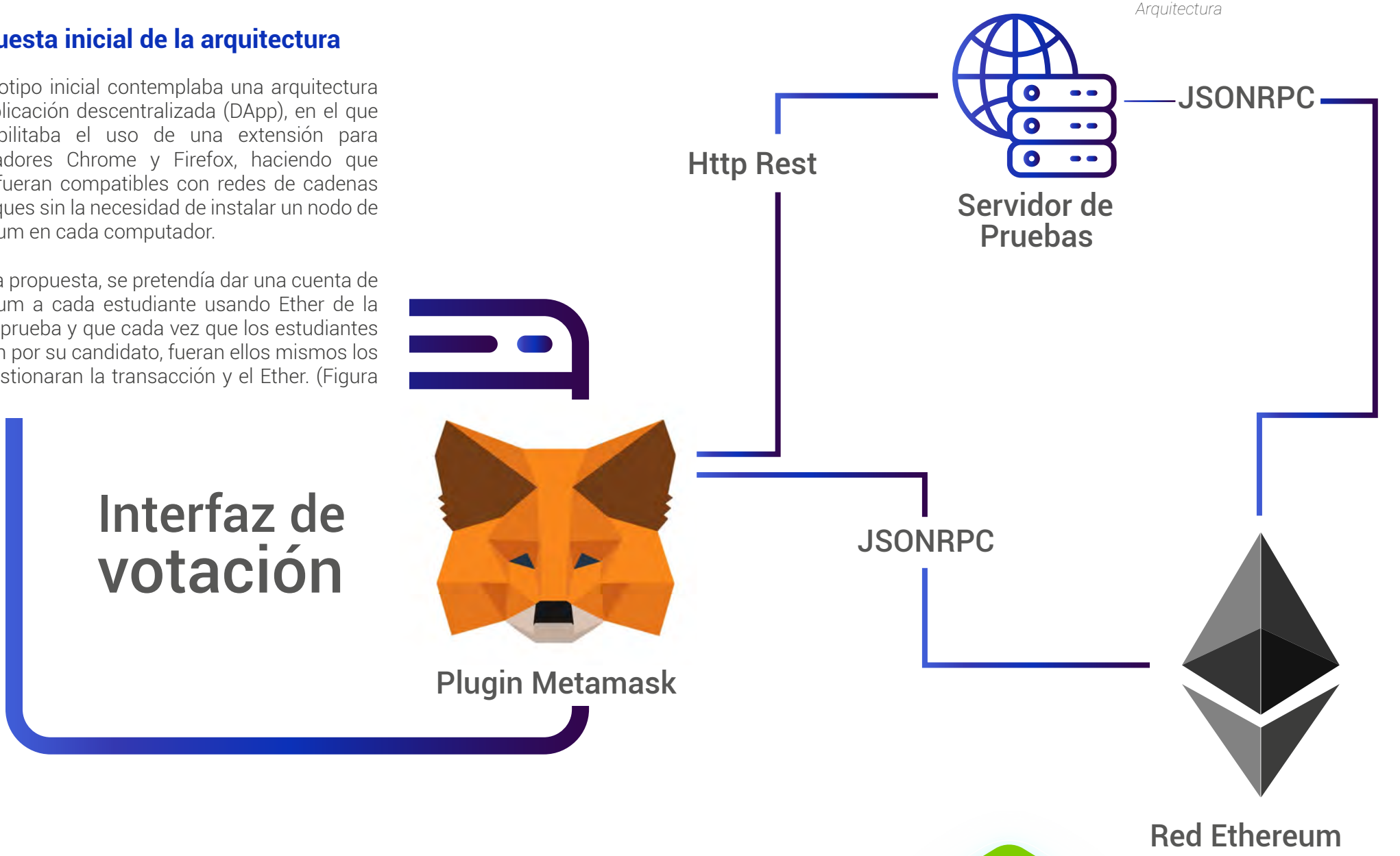
2.2

Propuesta inicial de la arquitectura

El prototipo inicial contemplaba una arquitectura tipo aplicación descentralizada (DApp), en el que se habilitaba el uso de una extensión para navegadores Chrome y Firefox, haciendo que estos fueran compatibles con redes de cadenas de bloques sin la necesidad de instalar un nodo de Ethereum en cada computador.

En esta propuesta, se pretendía dar una cuenta de Ethereum a cada estudiante usando Ether de la red de prueba y que cada vez que los estudiantes votaran por su candidato, fueran ellos mismos los que gestionaran la transacción y el Ether. (Figura 16)

Figura 16 Representación de la Arquitectura



2.3
Implicaciones jurídicas

Bajo el marco dispuesto por la ley 1581 de 2012 y su decreto reglamentario 1074 de 2015 de tratamiento de información, al igual que las leyes de protección del menor, teniendo en cuenta que existe información de carácter público, semipúblico y privado, se recomendó el tratamiento privado de fotografías de candidatos, sus nombres y apellidos y cualquier otra información que pudiese representar un riesgo a su integridad.

La legislación vigente relacionada con plataformas tecnológicas no aplica en sentido estricto para aplicaciones como las que se hacen sobre la red Blockchain, dado que la información se encuentra distribuida en diferentes nodos que no pueden ser auditados o revisados en un sentido estricto. Para poder realizar un manejo adecuado de los datos de los estudiantes, fue necesario hacer una modificación a la forma en que se desarrollaba la arquitectura de la aplicación. También se generó un contrato de protección de datos entre la Universidad Nacional y cada una de las instituciones educativas participantes de este proceso, para poder hacer uso de la información de cada estudiante para identificarlo ante el sistema como individuo único habilitado para votar

2.4
Visitas iniciales a colegios

El equipo de la Alcaldía de Bogotá, en compañía del ViveLab Bogotá realizaron una presentación para explicar a los colegios la estructura de la propuesta de elecciones con Blockchain, así como los compromisos y beneficios que debían asumir para formar parte de este ciclo, en el proceso se indaga sobre la experiencia en cada colegio en el desarrollo de elecciones con los estudiantes, para poder entender los inconvenientes que han tenido haciendo uso de herramientas tecnológicas y cómo los han podido solucionar. A continuación, se presenta un resumen de las visitas a cada IED participante:

Colegio Unión Colombia IED

La reunión se realizó el día 29 de enero de 2018, dentro de los acuerdos estuvo realizar una reunión el 7 de febrero para validar el proceso de votaciones con el prototipo navegable, a las 2:20 pm. El profesor encargado del proceso dentro del colegio se comprometió a compartir una lista con los datos de los estudiantes que iban a participar del proceso electoral.

En ese mismo día se realizaron algunas aclaraciones técnicas y logísticas, asimismo se aclara que el proceso de elecciones de representantes estudiantiles debe ocurrir antes del 21 de febrero de acuerdo con las directrices de la Secretaría Distrital de Educación. Y se acordó realizar las votaciones con estudiantes de grados 9°, 10° y 11°.

Colegio Rafael Bernal IED.

La reunión se realizó el día 31 de enero de 2018, los representantes del Colegio en la reunión comparten el proceso que están planeando que implica la solicitud de cubículos a la registraduría para facilitar las elecciones. Al final de la reunión se acordó programar una nueva reunión con la Coordinadora de primaria para el desarrollo de las elecciones con estudiantes de grados 3°, 4° y 5°.

En la segunda reunión realizada el día 6 de febrero, se realizó la misma presentación y propuesta con la coordinadora de la sección primaria, al final se acordó realizar el proceso con los grados 3° y 4°, la coordinadora al final se comprometió a pasar la lista de los estudiantes para las votaciones.

Colegio El Rodeo IED.

La reunión se realizó el día 31 de enero de 2018, el profesor encargado del proceso en el colegio se comprometió a facilitar la lista de los estudiantes y candidatos con sus respectivas fotos. Se acordó realizar elecciones de gobierno escolar para todos los estudiantes de la institución a través de

la aplicación con tecnología Blockchain y realizarlas el mismo día en las dos sedes físicas de la institución educativa.

2.5
Red-P

Por la naturaleza del prototipo Blockchain se requirió de equipos de cómputo en las IED con acceso a Internet que permitieron ingresar a la página de pruebas que se encontraba alojada en el siguiente dominio:

https://votacion.vivelabbogota.com.

Por tal motivo fue necesario hacer una solicitud formal a RED-P por medio de la Alta Consejería Distrital de TIC con el fin de habilitar el uso de este dominio en los equipos de las IED, esta solicitud fue tramitada con éxito y en el tiempo estipulado en dos de las IED, en la tercera no fue posible realizar la actividad en las fechas adecuadas de las elecciones de representante estudiantil por tanto fue necesario hacer de manera posterior el proceso electoral.

2.5.1
Pruebas en Instituciones Educativas Distritales

Para validar la correcta funcionalidad del prototipo en los equipos de cómputo de cada uno de los colegios, se tuvo contacto con una persona encargada de las salas de informática para verificar el acceso al internet de la página donde se iban a realizar las votaciones. Estas personas debían tener acceso a los equipos que se iban a disponer para la realización de las votaciones y debían entrar a la página solicitada para verificar que Red-P no tuviera el dominio bloqueado.

Figura 17. Equipo de cómputo del Colegio Unión Colombia - Aún sin acceso al dominio.

2.6
Pruebas preliminares

Durante el desarrollo del prototipo se realizó una validación inicial de la funcionalidad con 4 candidatos potenciales a la presidencia de Colombia (en ese momento), esta validación se llevó a cabo con la mayoría de los integrantes presentes en el laboratorio de ViveLab.

Se dispuso un computador para realizar la prueba, pero antes de que cada participante fuera a votar con su número de identidad correspondiente, se les pidió el favor de hacer la misma votación en tarjetones de papel para al final verificar que la cantidad de votos fuera la correcta y el número de votos por cada candidato, concordara con los registrados a mano en los tarjetones.

En total fueron 20 participantes que votaron durante la prueba realizada, posteriormente se comprobó la concordancia con los tarjetones en papel y así se verificó la garantía de los resultados que se pueden obtener a través del uso del prototipo de Blockchain.


```
[
    {
        "id": "651651651",
        "fname": "Iván",
        "lname": "Duque",

        "votes": "5",
        "nomination": "procurator"
    },
    {
        "id": "516561",
        "fname": "Alejandro",
        "lname": "Ordoñez",

        "votes": "3",
        "nomination": "procurator"
    },
    {
        "id": "5651651",
        "fname": "Vargas",
        "lname": "Lleras",

        "votes": "2",
        "nomination": "procurator"
    },
    {
        "id": "4516531651",
        "fname": "Marta",
        "lname": "Ramirez",

        "votes": "10",
        "nomination": "procurator"
    }
]
```


Figura 18. Formato JSON de los resultados obtenidos en la prueba interna.

2.7
Implementación del prototipo

El desarrollo del prototipo se guio bajo la propuesta inicial de la arquitectura, haciendo énfasis en el desarrollo del contrato inteligente de votaciones, e implementación de la DApp (Aplicaciones Descentralizadas). Sin embargo, dadas las recomendaciones y restricciones de índole jurídica, se determinó que la arquitectura inicial propuesta no era conveniente ya que exponía públicamente información de los sufragantes y candidatos, al igual que una posible trazabilidad de su votación.

Lo anterior obligó a un replanteamiento del contrato inteligente de votación, en el que el modelo de un estudiante con cuenta se eliminó, y se delegó la responsabilidad al colegio de lidiar con dichas transacciones, así se creaba únicamente una cuenta de Ethereum por colegio y en unas estructuras internas, se almacenaban los candidatos, los sufragantes y sus votos, sin que ello revelara la intención de voto, pero permitiendo contabilizar dicho voto al candidato elegido, y certificando que el sufragante ejerció su derecho al voto.

Estas nuevas consideraciones, obligaron a replantear también la forma en la que los distintos componentes se conectaban, eliminando la dinámica en la que el navegador instalaba el plugin de metamask y dejando la responsabilidad de lidiar con las transacciones a un Back-end que se comunicaba directamente con la cadena de bloques. (Figura 21)

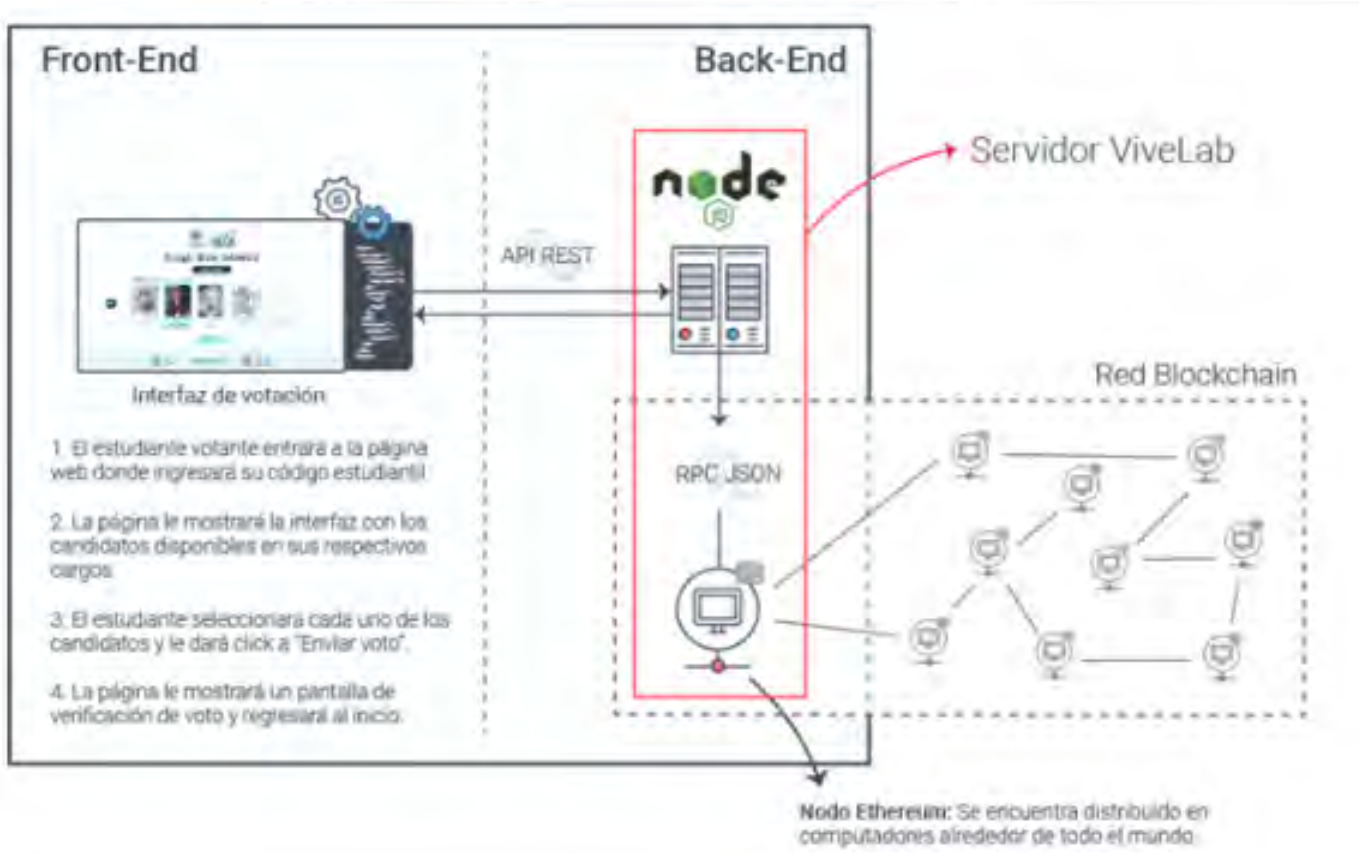


Figura 19.. Esquema de funcionamiento del prototipo

2.7.1
Desarrollo del contrato inteligente

En una versión inicial del desarrollo del contrato inteligente, se pensaba que el sufragante iba a manejar su cuenta y su intención de voto, y esto suscitó que el desarrollo del contrato siguiera una línea en la que todas las decisiones estaban directamente relacionadas con la cuenta del sufragante. Esta primera versión del contrato inteligente permitió validar conceptos de programación de contratos inteligentes y su relación con las cuentas de los sufragantes.

Sin embargo, las consideraciones logísticas y jurídicas replantearon el esquema, donde las cuentas se manejaban por colegio. Esto obligó a que se modelaran estructuras de datos, donde el colegio apareciera como entidad superior que contenía colecciones de candidatos y sufragantes, y certificados de votación. Para la estructura del candidato se establecieron datos básicos como nombre, apellido, curso, programa de gobierno, cargo al que se postulaba y total de votos obtenidos. Para el sufragante sólo se necesitaba el código estudiantil.

Cuando un sufragante votaba, el voto se registraba en una estructura que enlazaba el cargo por el cual votaba y las fecha y hora en la que votó, dando lugar a la generación del certificado. Paralelamente el voto se contabilizaba en la estructura de candidato, todo ello sin que se relacionara al sufragante y su intención de voto.

2.7.2
Desarrollo del front end

El front end se desarrolló usando VueJS (un framework JavaScript) al que se le inyectó Web3 (el API JavaScript de Ethereum Foundation para manipulación de la cadena de bloques de Ethereum con el protocolo JSON RPC) y truffle-contract (un encapsulador de utilidades para manipular el código del contrato inteligente en código de JavaScript). El desarrollo integraba el plugin de MetaMask para el navegador, permitiendo que la cuenta del sufragante interactuara directamente con el contrato inteligente en la cadena de bloques.

En el cambio exigido por las implicaciones jurídicas y logísticas, se migraron las funcionalidades de Web3 y truffle-contract a un back end usando ExpressJS (ver el apartado Desarrollo del back end). Para la conexión del Front-end con el Back-end se usó una comunicación HTTP por servicios REST con la librería Axios (librería de utilidades de comunicación HTTP), integrado a un estado global de la aplicación administrado con Vuex (administrador de estados y librería para VueJS), permitiendo una programación reactiva (un paradigma de programación que se enfoca en el flujo de datos y la propagación de cambio).

2.7.3
Desarrollo del back end

En la implementación del Back-end se diseñó una arquitectura que no usaba el plugin de Metamask, y se diseñó un API Rest con los siguientes requerimientos:

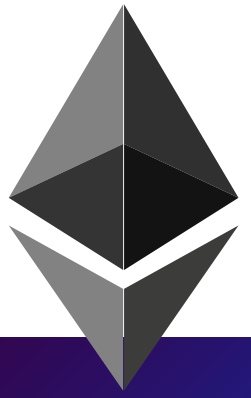
- Una aplicación que se ejecutara en NodeJS.
- Uso de ExpressJS que es un framework en Javascript para desarrollar aplicaciones en backend.
- Uso deTruffle framework para desarrollar aplicaciones sobre la red Ethereum.

Los servicios creados a partir de ExpressJS ejecutan las peticiones realizadas por el Front-end para que sean redireccionadas como invocaciones RPC en formato JSON con las librerías Web3 y truffle-contract a una dirección de contrato (address contract) donde está desplegado el contrato inteligente. Para acceder a la red pública de Blockchain, se usó el framework de truffle para compilar y desplegar el contrato a través de un nodo de Ethereum que se instaló en los servidores de VIvelab.

El contrato inteligente que se ha desarrollado en Solidity se compila y luego se despliega en el nodo

de Ethereum, en la versión de desarrollo se usó como nodo de prueba de Ethereum, TestRPC que es un cliente de Ethereum para pruebas, o para desplegar en la red pública a través de un nodo parity.

2.7.4
Despliegue del nodo de Ethereum



Cuando se intenta desplegar un nodo público de Ethereum, hay muchos problemas, lo que provoca una gran demora en el desarrollo. Las razones son:

- Se requieren horas y días sincronizando el cliente Go de Ethereum para comenzar el desarrollo de Ethereum, se necesita sincronizar todo el Blockchain que se encuentra en varios GB en este momento.
- La sincronización es muy lenta, puede tardar muchísimas semanas a pesar de tener un Internet muy rápido.
- Muchos errores de sincronización la detienen y hay que comenzar desde cero.
- Demasiada confusión con respecto a desplegar las redes de prueba Ropsten, Kovan o Rinkeby, ya que la aplicación Ethereum Wallet & Mist no muestra el nombre de la red de prueba fácilmente.

Parity permite desplegar un nodo de Ethereum y está diseñado para superar mucho de los problemas que se han mencionado. No solo sincroniza todo rápidamente, sino que también ofrece un navegador Dapp y una interfaz web para interactuar con la red Ethereum.

Actualmente, Parity está disponible en Ubuntu, Mac, Windows y Docker. También es necesario instalar geth y ethminer para minar eth de prueba para el proceso.

2.7.5
Dificultades técnicas

El equipo de desarrollo ya tenía cierta experiencia con el desarrollo de DApps, integrando el desarrollo de aplicaciones front end con frameworks JavaScript modernos (como ReactJS, VueJS, y en menor grado AngularJS) y Web3, truffle-contract y su debida programación de contratos inteligentes con Solidity para la cadena de bloques de Ethereum. Esto fija como punto de partida el conocimiento de que Web3, al ser un API JavaScript con protocolo de comunicación JSON RPC, exige un ambiente de desarrollo de aplicaciones con JavaScript, usando un back end JavaScript. Como resultado de una investigación en la que se buscaba usar una solución JavaScript pero que permitiera comunicaciones HTTP REST para servir al front end se decidió usar ExpressJS.

Este cambio también obligó a que en el nuevo back end se implementaran estrategias de administración de cuentas que en el ambiente previo eran responsabilidad del plugin de MetaMask, específicamente con lo relacionado a la apertura y cierre de permisos de uso de la cuenta. Por ello, se desplegó un nodo de Ethereum con los permisos necesarios para recibir comandos administrativos para desbloquear la cuentas. Estos comandos se invocan a través de peticiones JSON-RPC, desde el back-end.

El poco conocimiento de la herramienta obligó a montar el backend como una aplicación monolítica, sin segmentaciones lógicas de controladores, modelos, servicios o motores y un acceso a datos, precisamente la capa de acceso a la cadena de bloques. Esto deja la deuda técnica de segmentar el monolito en capas lógicas en una arquitectura más robusta.

Para la programación del contrato inteligente se usó Solidity, un lenguaje orientado a contratos creado en agosto de 2014, y que a la fecha de esta escritura está en la versión 0.4.21. Evidentemente es un lenguaje de propósito general muy joven si se compara con otros lenguajes de programación,

y que por lo tanto priva al desarrollador de herramientas comunes para resolver problemas usando patrones conocidos. Un ejemplo específico es la carencia de una estructura de control switch, obligando a desarrollar un bloque de código similar con una serie de condiciones if-else encadenadas.

El contrato inteligente asociado a las votaciones fue desplegado en una red de prueba de Ethereum, que tiene todas las prestaciones de la red real, sin embargo, y por las condiciones propias de una red de prueba, hay elementos que no se pueden usar a voluntad, como el caso del precio del gas que se está dispuesto a pagar en aras de acelerar el tiempo de minado de dichas transacciones.

Con el volumen de transacciones que se generaron se tuvieron demoras en el minado, lo que repercutió en el tiempo de confirmación de los candidatos ganadores. Estos tiempos dependen de la cantidad de gas asignado para la ejecución de la transacción, en Ethereum el gas es algo similar a las tarifas de transacción en Bitcoin. Cada operación en la red Ethereum requiere una cantidad no modificable de gas, por ejemplo agregar dos números cuesta 3 de gas, calcular el hash cuesta 30 de gas, y el envío de una transacción cuesta 21,000 de gas. El gas se paga en Ether, simplemente se calcula una tasa de cambio de Gas/Ether cuando se envía una transacción en la cadena de bloques de Ethereum.

En el caso del proceso de votaciones este proceso de minado puede tomar de 20 a 180 segundos dependiendo del tráfico en la red pública de Ethereum.

2.8
Consideraciones logísticas

Al tratarse de un proceso electoral que implicaba la participación de varios estudiantes, fue necesario establecer un mecanismo de control, en primera instancia se verificaba el nombre y el código del estudiante en un listado impreso, y enseguida se le permitía el ingreso al área de votación (sala de informática con equipos dispuestos para tal fin), para identificar con claridad quiénes ya habían votado y quiénes hacían falta. Al final se hizo un recuento comparativo entre el total de los estudiantes que realizaron el voto y la cantidad de registros en el prototipo Blockchain.

Para el desarrollo del proceso electoral en el colegio Rafael Bernal y el Rodeo, fue necesario acompañar con facilitadores de la Alcaldía de Bogotá y del equipo ViveLab el proceso con los estudiantes, esto debido a que para realizar la votación estaba planeado que ellos mismos ingresaran el código que los identificaba en el colegio, sin embargo, cada estudiante se identificaba por el curso y el número que tenía asignado en la lista correspondiente al curso, algunos de ellos (los más pequeños) no tenían claro cuál era su código, a medida que iban ingresando a votar, los facilitadores les ayudaban a digitar el código con un formato especial y posteriormente ellos seleccionaban el candidato por el que querían votar y finalmente enviaban su voto.

Figura 20. Proceso de votaciones colegio el Rodeo - 4 facilitadores, 1 por estudiante.

3. Resultados

3.1 Prototipo Final

A continuación, se muestran las principales páginas de la plataforma. Para ingresar al prototipo, se hizo desde la página web:

http://votacion.vivelabbogota.com,

en ella se encontraba un módulo administrativo para dar inicio al proceso de votación para cada Institución Educativa, en seguida cada estudiante era identificado con un código único que se componía de diferentes variables, ejemplo AM6011, este código se leía de la siguiente forma: M - Jornada de la Mañana, A - Sede a la que pertenece, 601 - curso seiscientos uno, 1 - el primer estudiante de la lista (Figura 21).

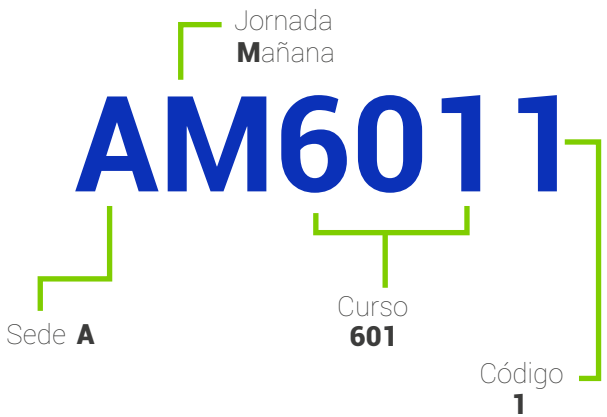


Figura 21. Explicación de la configuración del código de cada estudiante frente al sistema

3.1.1 Página de identificación

El estudiante debió escribir su número de identificación que en este caso corresponde al código descrito en la figura 21, cuando la caja de texto esté vacía, el botón de ENTRAR A VOTAR estará deshabilitado.

Figura 22.. Pantalla de registro de código de estudiante

3.1.2
Página de votación

En la página de votación, el estudiante vio su nombre y se le pidió que seleccionara un candidato por quién votar, al igual que en la página de identificación, el botón está deshabilitado hasta que no se seleccione un candidato para cada cargo definido previamente con la institución. Al hacer clic en enviar voto, se mostró un mensaje de confirmación antes de poder enviar el voto (Figura 23).

Figura 23. Candidatos reales para personero del colegio Rafael Bernal IED

3.1.3
Página de votación exitosa

Una vez que el sistema registró el voto, se presentó un mensaje que indicó la validez del mismo.

Figura 24. Pantalla de verificación del envío de un voto

3.1.4
Video demostrativo

La funcionalidad del prototipo se muestra en el siguiente link que conduce a un video demostrativo del paso a paso que realizaban los estudiantes al momento de votar:

https://drive.google.-com/open?id=1UuIrn-QOa3oELIfxO4w-w6JdU-tOulwYrE

3.2
Validación en las Instituciones Educativas Distritales

El proceso de votación se realizó en los colegios Rafael Bernal Jiménez IED y El Rodeo IED, se logró registrar con éxito un total de

1429 votos
de estudiantes,

cuyo proceso se llevó a cabo en 2 jornadas los días 22 y 23 de febrero.

En el colegio **Rafael Bernal Jiménez,** se registraron un total de 205 estudiantes habilitados para votar, los cuales pertenecen a los grados tercero y cuarto de primaria, la prueba del prototipo se realizó en la jornada de la mañana del día jueves 22 de febrero en aproximadamente tres (3) horas.

En el colegio **El Rodeo IED**, se registraron un total de 1223 estudiantes habilitados para votar, dada la cantidad de estudiantes, fue necesario realizar la votación en las jornadas de la mañana y la tarde en dos sedes al mismo tiempo, el día viernes 23 de febrero.

Para el Colegio **Unión Colombia** no fue posible realizar las votaciones debido a un retraso en la configuración de la RedP que impedía el acceso a la web de votación para la fecha establecida de las elecciones. Por lo tanto, el equipo se comprometió a realizar un taller con un curso a la entidad educativa, para explicar el potencial de la tecnología y hacer una demostración con una votación de prueba dentro del mismo taller.

3.2.1
Colegio RAFAEL BERNAL JIMENEZ IED

A continuación, se presentan los datos que identifican al colegio y la información requerida para el proceso de votación, cabe resaltar que los resultados obtenidos a través de Blockchain fueron un segmento de la votación completa que se desarrolló de forma tradicional empleando tarjetas en papel y material de apoyo de la registraduría.

DATOS COLEGIO:
Dirección: Carrera 53 # 75-17 (Sede A - Principal)
Localidad: Barrios Unidos
Teléfonos: 2509780 / 2315078 / 6602933

DATOS RESPONSABLE:
Nombre: Dora María Cuervo
Cargo: Coordinadora sección primaria
Correo: doracrow08@yahoo.es

3.2.1.1
Logística

l proceso electoral se desarrolló en la jornada de la mañana del 22 de febrero de 2018 con los cursos de 3° y 4° grado, con un total de 6 salones y 205 estudiantes registrados para la votación.

El proceso se inició bajo la intención de trabajar en 10 computadores, situación que no fue posible por la edad de los estudiantes y la capacidad reducida de personal para facilitar la identificación de cada estudiante con su código personal, se desarrolló en 5 computadores con sistema operativo Windows, navegador Chrome y conexión a Internet.

Desarrollo de la votación:

- Llamado de los estudiantes junto con el docente encargado.
- Organización de los estudiantes por orden de lista.
- Formación en el exterior de salón y paso de los estudiantes en grupos de 5 personas.
- Validación de la identidad de los estudiantes con un listado impreso.
- Asignación del código de votación a cada estudiante (curso + código de estudiante).
- Apoyo de los facilitadores para registrar en el sistema el código de cada niño y explicar los pasos del proceso.

El proceso comenzó a las 8:00 am y tuvo una duración aproximada de 3 horas, al final del día se verificó la totalidad de las transacciones y se envió el resultado a la encargada del colegio.

3.2.1.2 Evidencias

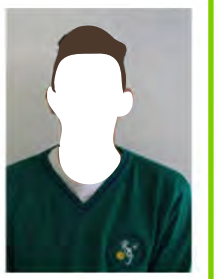
Figura 25. Proceso electoral y facilitación con estudiantes del Colegio Rafael Bernal IED

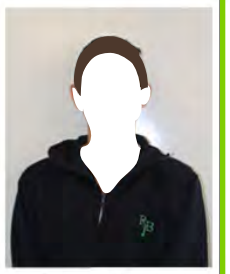
Figura 26. Estudiante realización votación en el colegio Rafael Bernal IED

Figura 26. Estudiante realización votación en el colegio Rafael Bernal IED

3.2.1.3
Candidatos

Personería


1. Jesid Villalobos


2. Andres Narvaez


3. María León


4. Enderson Stiven

Contraloría

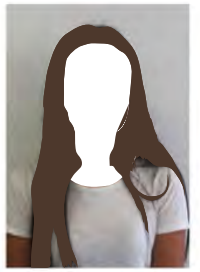

1. Esteban Sosa


2. Laura Sanchez


3. (Sin Nombre)


4. Juan Alzate

Cabildante


1. Yulieth Peña

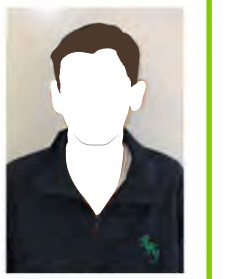

2. Ana Torres

Veeduría

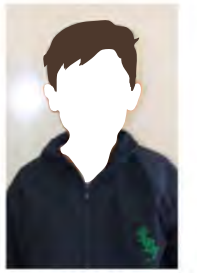

1. (Sin Nombre)

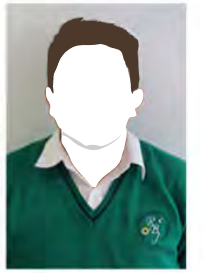

2. Stiward Mosquera


3. Johan Hernandez


4. David Romero

Vigía Ambiental


Juan León


Juan Lara


Santiago Torres

Nota:
El tarjetón número 3 de Contraloría no registra nombre pero si foto, esto debido a la información incompleta recibida por parte del responsable del colegio. Lo mismo ocurre con el tarjetón número 1 de Veeduría que al igual no registra foto y tampoco nombre.

3.2.1.4 Resultados

A continuación, se muestran los resultados obtenidos del prototipo de Blockchain de acuerdo con cada cargo registrado junto con el candidato correspondiente, al final se muestra la cantidad de votos en blanco y total de votos registrados.

Candidato	Personería	Contraloría	Cabildante	Veeduría	Vigía Ambiental
Jesid Villalobos	32				
Andrés Narvaez	26				
María León	97				
Enderson Stiven	34				
Esteban Sosa		56			
Laura Sánchez		32			
N/A (Con foto)		50			
Juan Alzate		51			
Yulieth Peña			107		
Ana Torres			78		
N/A				2	
Stiward Mosquera				43	
Johan Hernandez				93	
David Romero				49	
Juan León					79
Juan Lara					57
Santiago Torres					51
Voto en Blanco	1	1	5	3	3

Total Votantes:

190

3.2.2
Colegio EL RODEO IED

A continuación, se muestran los datos que identifican al colegio y la información requerida para el proceso de votación. El colegio El Rodeo se divide en dos sedes y dos jornadas, es decir que la numeración de los cursos en la jornada de la mañana y la tarde fue la misma, por lo que fue necesario identificar sede y jornada, adicional al código del curso y del estudiante.

DATOS COLEGIO:
Dirección: Calle 40A SUR # 2-56 ESTE (Sede A - Principal)
Localidad: San Cristóbal
Teléfonos: 2068049 / 3638423

DATOS RESPONSABLE:
Nombre: Víctor Hugo Chacón
Cargo: Rector
Correo: victorchac@yahoo.es

3.2.2.1
Logística

El proceso electoral se desarrolló en las jornadas de la mañana y de la tarde del 23 de febrero de 2018 con los cursos de 3° a 11° grado, con un total de 33 salones y 1223 estudiantes registrados para la votación repartidos de la siguiente manera: Sede A en la jornada de la mañana: 14 cursos con un total de 543 estudiantes, Jornada de la tarde: 13 cursos con un total de 471 estudiantes, Sede B en la jornada de la mañana: 3 cursos con un total de 105 estudiantes, y en la jornada de la tarde 3 cursos con un total de 104 estudiantes.

El proceso se desarrolló en ambas sedes al mismo tiempo, en la sede A se dispuso de 4 computadores y 4 facilitadores que estaban recibiendo a cada uno de los estudiantes que iban entrando a votar con su correspondiente código.

El proceso consistía en ir llamando a cada curso con su profesor a cargo para que ordenara a sus estudiantes por número de lista, los niños realizaban una fila afuera de la biblioteca donde se estaba realizando la votación e iban ingresando en grupos de 4.

Desarrollo de la votación:

- Llamado de los estudiantes junto con el docente encargado.
- Organización de los estudiantes por orden de lista.
- Formación en el exterior del salón y paso de los estudiantes en grupos de 4 (Sede A) o 5 (Sede B).
- Validación de la identidad de los estudiantes con un listado impreso.
- Asignación del código de votación a cada estudiante (curso + código de estudiante).
- Apoyo de los facilitadores para registrar en el sistema el código de cada niño y explicar los pasos del proceso.

El proceso comenzó a las 8:00 am y tuvo una duración aproximada de 4 horas en la mañana, en la tarde la duración fue aproximadamente de 3 horas. Por la cantidad de transacciones y el tiempo que estas requirieron para ser verificadas en la red Blockchain, fue necesario esperar hasta el siguiente día para entregar los resultados.

3.2.2.2
Evidencias

Figura 29. Desarrollo proceso electoral en colegio El Rodeo Sede A

Figura 30. Desarrollo proceso electoral en colegio El Rodeo Sede A

Figura 32. Estudiantes votando en colegio El Rodeo Sede A

Figura 31. Estudiante votando en colegio El Rodeo Sede A

3.2.2.3 Candidatos

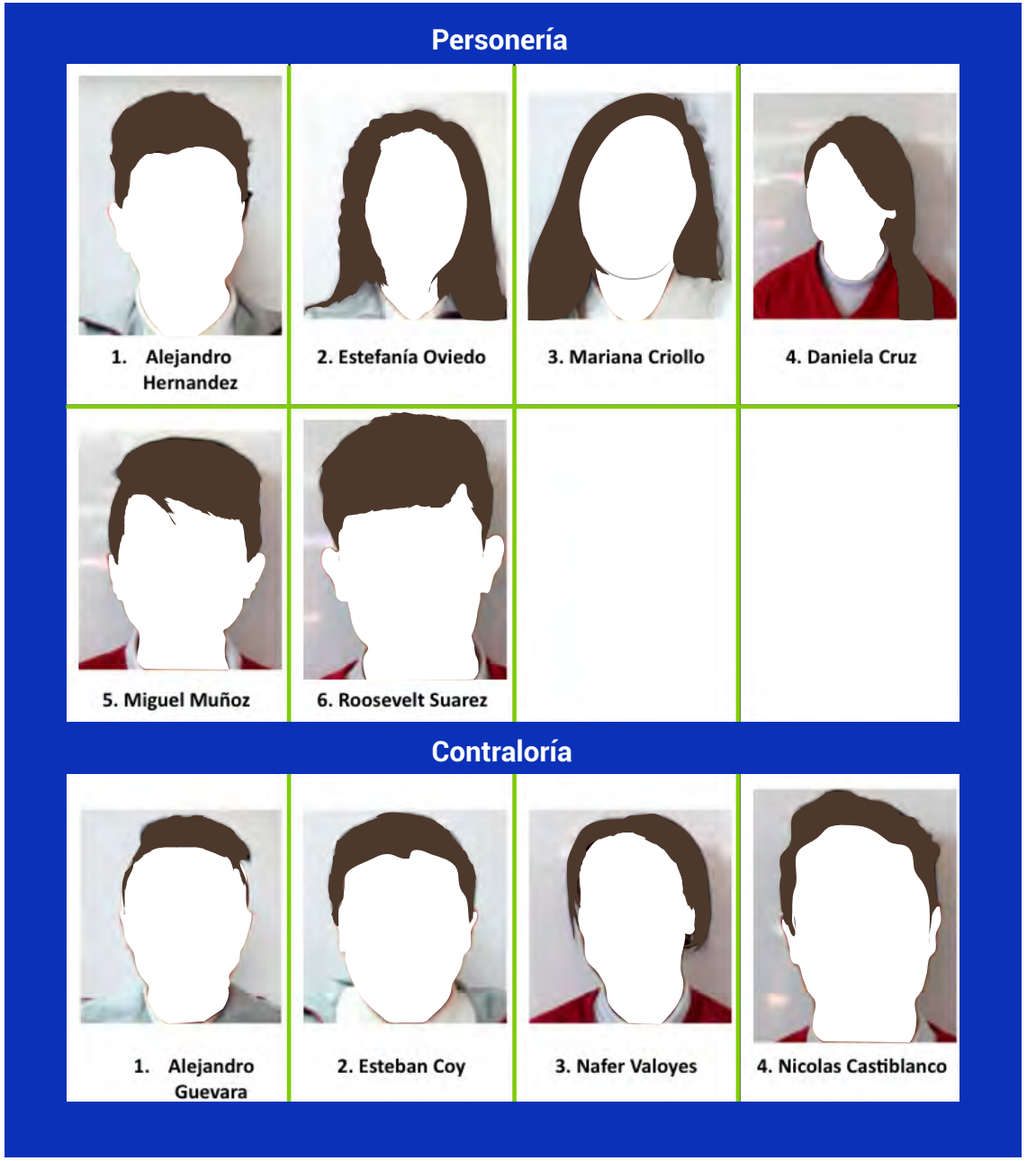


Figura 33. Fotos reales de los candidatos (Información de carácter sensible)

3.2.2.3 Resultados

A continuación, se muestran los resultados obtenidos del prototipo de Blockchain de acuerdo con cada cargo registrado junto con el candidato correspondiente, al final se muestra la cantidad de votos en blanco y total de votos registrados.

Candidato	Personería	Contraloría
Alejandro Hernandez	248	
Estefania Oviedo	244	
Mariana Criollo	86	
Daniela Cruz	242	
Miguel Muñoz	143	
Roosevelt Suarez	86	
Alejandro Guevara		306
Estevan Coy		155
Nafer Valoyes		173
Nicolas Castiblanco		366
Voto en Blanco	70	119

Total Votantes:

1119

3.2.3
Colegio UNION COLOMBIA IED

La votación en el colegio Unión Colombia no fue posible, debido a un retraso en la configuración de la RedP que impedía el acceso a la web de votación para la fecha establecida de las elecciones. Por lo tanto, el equipo Blockchain se comprometió a realizar un taller con un curso de la entidad educativa para explicar el potencial de la tecnología y hacer una demostración con una votación de prueba dentro del mismo taller.

DATOS COLEGIO:
Dirección: Cra 7A # 182A-07
Localidad: Usaquén
Teléfonos: 6796956

DATOS RESPONSABLE:
Nombre: Martha Venegas
Cargo: Rectora
Correo: mcvenegas86@gmail.com

3.2.2.1
Logística

El taller se realizó el día miércoles 14 de marzo a las 5:15pm, tuvo una duración de 1 hora. El curso seleccionado por el docente Julián Cárdenas fue 1101 (11A) con un total de 32 estudiantes asistentes.

Los temas desarrollados durante el taller fueron:

- Una reflexión sobre la seguridad y transparencia de las votaciones electorales.
- Breve explicación de las redes descentralizadas.
- Introducción a la tecnología Blockchain.
- Demostración del prototipo funcional para votaciones en Blockchain.
- Ejemplo de prueba con candidatos presidenciales.

3.2.3.2
Evidencias

Figura 34. Taller con estudiantes del colegio Unión Colombia IED

Figura 35. Taller con estudiantes del colegio Unión Colombia IED

Figura 36. Taller con estudiantes del colegio Unión Colombia IED

Figura 37. Taller con estudiantes del colegio Unión Colombia IED

3.2.3.3
Candidatos

Figura 38. Listado de candidatos presidenciales para ejercicio electoral

3.2.3.4
Resultados

A continuación, se muestran los resultados obtenidos del prototipo de Blockchain, demostración funcional realizada durante el taller con candidatos presidenciales.

Candidato	Presidencia
Germán Lleras	0
Gustavo Petro	15
Humberto de la Calle	0
Iván Duque	7
Juan Pinzón	0
Piedad Córdoba	2
Sergio Fajardo	1
Viviane Morales	2
Voto en Blanco	5

Total Votantes:

32

Tabla 3. Resultados elecciones Colegio Unión Colombia

3.2.3.3
Evidencias de transacciones

De acuerdo con la figura 39, existen varios elementos que componen la transacción que está registrada en la red pública de Blockchain. Se enumeran de la siguiente forma:

- **TxHash:** Es el identificador de la transacción dentro de la cadena de bloques de Ethereum y se genera con un proceso matemático que toma una cantidad variable de datos y produce una salida más corta de longitud fija.
- **TxReceipt Status:** Estado de la transacción.
- **Block Height:** El número de bloque en el que se incluyó la transacción.
- **Timestamp:** La fecha en que se minó el bloque y la transacción fue registrada en la cadena de bloques.
  From: La dirección de Ethereum que envía la transacción.
- **To:** La dirección de Ethereum que recibe la transacción, que en este caso es la dirección del contrato inteligente.
- **Value:** La cantidad de éter que fue enviado y el equivalente en USD.
- **Gas Limit:** La cantidad máxima de gas que el emisor está dispuesto a comprar para la transacción.
- **Gas Used By Txn:** La cantidad real de gas utilizada para la transacción.
- **Gas Price:** El precio del gas en Ether. El precio del gas lo deciden los mineros. (Un GWei es 10 ^ 9 Wei o 10 ^ -9 Ether).
- **Actual Tx Cost/Fee:** Gas usado x Costo de gas
  Nonce: Un número secuencial vinculado a cada transacción que representa el número de transacciones que la cuenta del remitente ha realizado en la red. Entonces, por ejemplo, la primera transacción que una cuenta envía tendrá un nonce de 0, la segunda será un nonce de 1, y así sucesivamente.
- **Input Data:** Un campo que es una cadena de bytes del contrato o de la transacción.

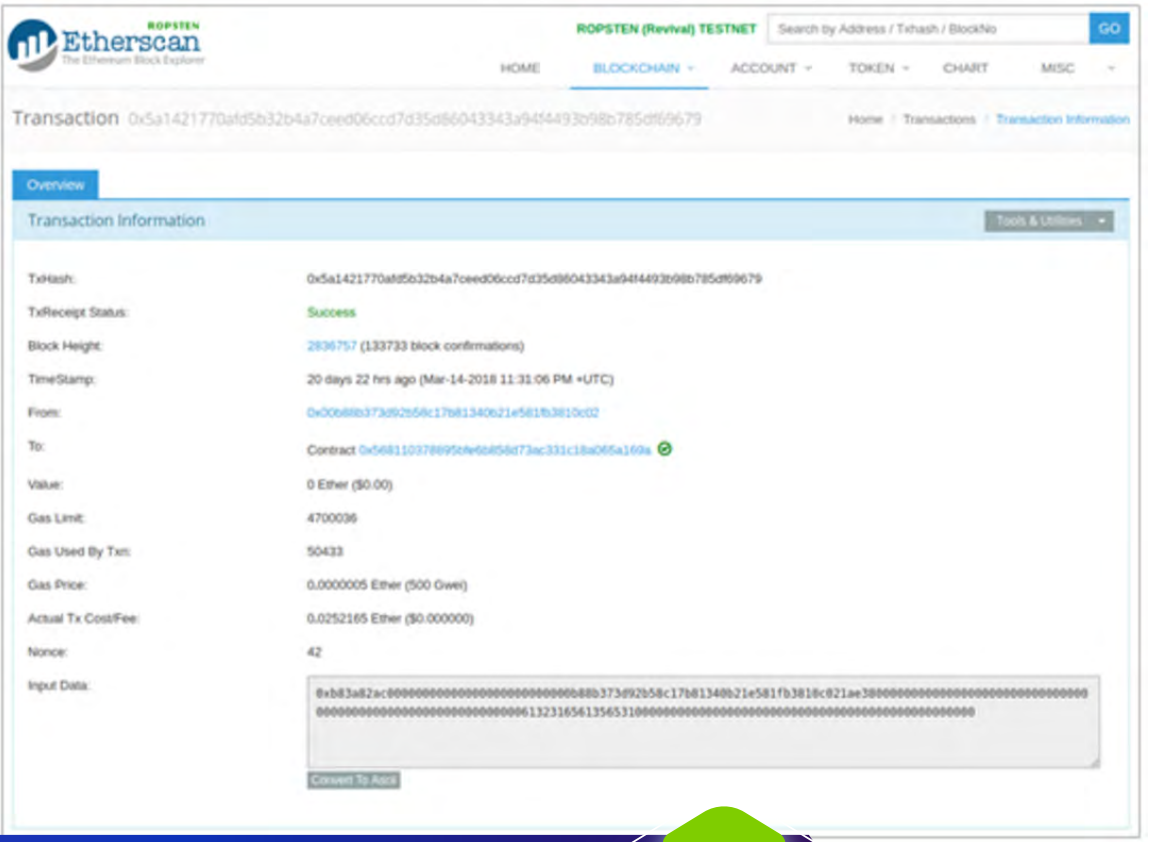


Figura 39. Página web Etherscan

3.3 Aprendizajes

El desarrollo del prototipo resaltó aspectos que se pueden profundizar para implementar arquitecturas más robustas, explorando diversas configuraciones que permitan abordar diferentes problemas. Salir de un estilo de programación orientado a aplicaciones descentralizadas usando el navegador y un plugin como puente de comunicación con la cadena de bloques, obliga a que las empresas o entidades exploren formas que involucren soluciones híbridas con bases de datos y almacenamiento de archivos binarios (imágenes, audios, videos, etc.), llevando a cadenas de bloques solamente información sensible que requiera ser auditada posteriormente.

4 Conclusiones

El uso de la tecnología Blockchain permite el desarrollo de procesos electorales ágiles y rápidos, desde el momento de la votación hasta el momento de consolidación de los resultados.

- La infraestructura de las Instituciones Educativas públicas permite el desarrollo de procesos electorales online, mientras que estos tengan una carga de recursos bien diseñada y ajustada a las capacidades de cada institución.
- La gestión de permisos con REDP puede ser un obstáculo para el desarrollo de este tipo de procesos cuando no se cuenta con un tiempo suficiente, una vez que se logra la apertura de las URL es muy sencillo realizar la aplicación de este tipo de pruebas.
- El ahorro de papel durante este tipo de procesos es uno de los logros más destacados por los docentes de las instituciones educativas participantes.
- La facilidad de registrar votos para estudiantes de grado 3, 4 y 5 hacen del proceso de elección digital una herramienta de valor para los docentes que garantiza la participación de los más pequeños.
- La logística de las votaciones y el tiempo empleado por los docentes y estudiantes para este proceso se optimiza, dado que un curso realiza su elección en un tiempo estimado de 10 a 20 minutos, cuando se tienen varios equipos disponibles para esta función.
- Es necesario contar con el apoyo de personas que ayuden a los estudiantes para identificarse frente a la plataforma de votación dado que el código de registro puede ser difícil de entender para algunos estudiantes.
- El tratamiento de datos de los estudiantes requiere que se realicen acuerdos entre las instituciones que organizan la votación y la institución educativa entendiendo que los participantes son menores de edad.
- En cada colegio los cargos de representante estudiantil tienen características específicas, por tanto, es necesario que la plataforma de votación se pueda personalizar, en cuanto al número de candidatos, la tipología de cargos a elegir, los nombres y fotografías de los candidatos y la base de datos de estudiantes habilitados para votar.
- Es posible que durante el proceso se presenten estudiantes que son nuevos en la institución y que no estén registrados en la base de datos de la misma, en estos casos es necesario contar con un mecanismo que permita ingresar estos estudiantes al sistema (equipo de soporte) o tener mecanismos alternos de votación (papeleta tradicional).
- Las legislaciones de los países, sobre todo latinoamericanos, no están preparadas para afrontar jurídicamente los escenarios que se presentan al implementar tecnologías emergentes, situación que nos lleva a hacer adaptaciones que cubren los procesos en el marco vigente (contratos de uso de datos para menores de edad).

- ✓ La arquitectura propuesta fue determinada por las restricciones logísticas y jurídicas, ya que para proteger la integridad de los niños se hizo necesario adoptar mecanismos que cifraran datos sensibles.
- ✓ La aplicación se desarrolló con una carga computacional fuerte al lado del backend, en aras de reducir el impacto de instalaciones al lado de los clientes. Esto redunda en una aplicación web de fácil acceso, que no requiere permisos excesivos, salvo garantizar que se puede acceder a su URL.

5 Alternativas de mejora del prototipo

- Este ejercicio evidenció falencias en la implementación de la solución basada en redes públicas de Blockchain, por ello es necesario hacer una investigación adicional del impacto del que puede ser objeto el rendimiento si la solución se implementa sobre redes privadas de cadenas de bloques.
- Como se ha dicho previamente, la logística implicaba tener a una persona verificando la identidad del estudiante para que este pudiera votar. Actualmente hay soluciones que se están desarrollando para solucionar el problema de la identidad digital, y se recomienda investigar en la integración de este tipo de soluciones para mitigar situaciones como la que se describe.
- Este tipo de propuestas aún requiere de muchas mejoras en relación con la identidad digital, el marco normativo y los costos asociados al uso de redes privadas de Blockchain aún hay un campo amplio de investigación antes de poder implementar procesos electorales de mayor escala.
- Para poder implementar este tipo de procesos en otras instituciones educativas se requiere de un equipo de soporte técnico y logístico que faciliten las labores de registro de votos y de personalización de la plataforma.

6 Retroalimentación

Desde la Alcaldía de Bogotá a través del ViveLab de la Universidad Nacional, demostramos que una tecnología emergente y compleja como lo es el Blockchain, puede resolver un caso real que enfrenta el sector público (educativo), como son las elecciones estudiantiles, y de esta forma evidenciamos los beneficios que trae esta tecnología innovadora para acercar a estudiantes y docentes, al mundo digital.

A pesar de que esta fue una prueba piloto, es importante la experiencia del equipo de trabajo y todo el insumo documental para replicar la estrategia, bien sea en esta o en futuras administraciones. La satisfacción de los más de mil 500 actores involucrados entre docentes, coordinadores y estudiantes frente a la aplicación del Blockchain en las elecciones estudiantiles, da cuenta de que estas estrategias acercan a la comunidad con la tecnología, en especial con aquellas que están emergiendo, fomentando así el aprendizaje e investigación desde temprana edad en las nuevas tendencias digitales.

A lo anterior y en aras de una posible nueva edición se debe agregar lo expresado en cuanto a la optimización del manejo y ahorro de recursos, como papelería, tiempo y dinero, lo que fortalecería la aplicación de una nueva elección de representantes estudiantiles basado en Blockchain.

Como siguiente paso se tiene planeado diferentes encuentros para socializar y exponer a la comunidad y principales actores interesados, los principales hallazgos del prototipo, así como los beneficios de la introducción de estos pilotos a eventos comunes que permitan la inclusión de la tecnología a la vida diaria y sus beneficios en los más pequeños.

7

Bibliografía

1. Bauerle, Nolan. (2017). What is a Distributed Ledger?. CoinDesk. Recuperado de https://www.coindesk.com/information/what-is-a-distributed-ledger/
2. Grant, T. (2016). R3 & Distributed Ledger Technology. In Focus, (Mayo). Recuperado de https://www.ecb.europa.eu/paym/pdf/infocus/20160422_infocus_dlt.pdf
3. Iansiti, M., & Lakhani, K. R. (2017). The Truth About Blockchain. Harvard Business Review, 95(1), 118-127. Recuperado de https://hbr.org/2017/01/the-truth-about-blockchain
4. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Recuperado de https://bitcoin.org/bitcoin.pdf
5. BTC Studios. (2017), Bitcoin can do smart contracts and Particl demonstrates how. Bitcoin Magazine by BTC Media LLC. Recuperado de https://bitcoinmagazine.com/articles/yes-bitcoin-can-do-smart-contracts-and-particl-demonstrates-how/
6. Digital.govt.nz. (2014-2018), Digital 5 (D5). New Zealand. Governance and Leadership. Recuperado de https://www.ict.govt.nz/governance-and-leadership/international-leadership/d5-wellington-2018/
7. Sulleyman, A (2017), Alphabay: Dark web drugs marketplace mysteriously goes offline sparking fears of a major heist. The Independent. Recuperado de http://www.independent.co.uk/life-style/gadgets-and-tech/news/alphabay-offline-dark-web-drugs-marketplace-bitcoin-major-heist-police-authorities-a7825696.html
8. Angel, M CV (2016), Kevin Mitnick, El hacker más famoso de la historia. Javaheros (Blog). Recuperado de https://javaheros.blogspot.com.co/2016/03/kevin-mitnick-el-hacker-mas-famoso-de.htm
9. Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187.
10. Brakeville, S., & Perepa, B. (2017). Blockchain basics: Introduction to distributed ledgers. developersWorks (IBM). Recuperado de https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/
11. The Linux Information Project. (2005), Timestamp Definition. Recuperado de: http://www.linfo.org/timestamp.html
12. Instant SSL (2017), What Is a Digital Signature? Comodo CA Limited. Recuperado de: https://www.instantssl.com/https-tutorials/digital-signature.html
13. Colombia. (1996). Ley general de educación. El pensador Editores. Recuperado de: https://www.mineducacion.gov.co/1621/articles-86240_archivo_pdf.pdf
14. SurBTC (2017). https://www.surbtc.com/colombia
15. R3 Blog (2017), Banco de la república colombia se vincula con r3 para fomentar innovación financiera. R3. Recuperado de:https://www.r3.com/blog/2017/08/29/banco-de-la-republica-colombia-se-vincula-con-r3-para-fomentar-innovacion-financiera/
16. Bitcoin. https://bitcoin.org/es/
17. Ethereum Foundation. https://www.ethereum.org
18. R3. https://www.r3.com
19. Aragon. https://aragon.one/
20. Ethereum community (2016). Contracts: What is a contract?. Recuperado de: http://www.ethdocs.org/en/latest/contracts-and-transactions/contracts.html
21. Ridley, M. (2017). The Bitcoin revolution is only just beginning. The Times. recuperado de: https://www.thetimes.co.uk/article/the-bitcoin-revolution-is-only-justbeginning-k9zj8cxnx
22. Treagust, S. (2017). 6 Business Benefits of Blockchain. The IFS Blog (IFS). Recuperado de:

https://blog.ifsworld.com/2017/06/6-business-benefits-of-blockchain/
23. Semana. (2017). Reinvención Digital de la Factura. Hablan las Marcas. Recuperado de: http://www.semana.com/hablan-las-marcas/articulo/facturas-electronicas/530368
24. Organisation for Economic Co-operation and Development. (2017). Blockchain Voting for Peace. Embracing Innovation in Government: Global Trends. Recuperado de: https://www.oecd.org/gov/innovative-government/embracing-innovation-in-government-colombia.pdf
25. Particl. https://particl.io/
26. Nxt. https://nxtplatform.org
27. QTUM Project. https://www.qtum.org/
28. RSK Labs. https://www.rsk.co/
29. Vitalik, B. (2013). Ethereum white paper: a next generation smart contract & decentralized application platform.
30. Vitalik, B. (2017). Notes on Blockchain Governance. Vitalik. Recuperado de: http://www.vitalik.ca/general/2017/12/17/voting.html
31. Ministerio de Educación Nacional de Colombia. (2010). ¿Qué es el Gobierno Escolar?. Recuperado de: https://www.mineducacion.gov.co/observatorio/1722/article-220386.html

8

Anexos

1. Anexo 1 Contrato Protección de datos - Colegio el Rodeo IED
2. Anexo 2 Contrato Protección de datos - Colegio Rafael Bernal IED
3. Anexo 3 Contrato Protección de datos - Colegio Unión Colombia
4. Anexo 4 Lista de estudiantes asistentes - Colegio El Rodeo IED
5. Anexo 5 Lista de estudiantes asistentes - Colegio Rafael Bernal IED
6. Anexo 6 Lista de estudiantes asistentes - Colegio Union Colombia IED
7. Anexo 7 Registro de transacciones - Colegio El Rodeo IED
8. Anexo 8 Registro de transacciones - Colegio Rafael Bernal IED
9. Anexo 9 Registro de transacciones - Colegio Union Colombia IED

Informe final

de resultados prototipo

Blockchain