# Tecnología Blockchain aplicada al voto electrónico

Jhon Alexander Carrión Piedra
*Facultad de la Energía*
*Universidad Nacional de Loja*
Loja, Ecuador
jhon.carrion@unl.edu.ec
0000-0003-4039-983X

Luis Xavier Paredes Cuenca
*Facultad de la Energía*
*Universidad Nacional de Loja*
Loja, Ecuador
luis.x.paredes@unl.edu.ec
0000-0002-8806-2710

Cristian Ramiro Narvaéz Guillen
*Facultad de la Energía*
*Universidad Nacional de Loja*
Loja, Ecuador
cristian.narvaez@unl.edu.ec
0000-0002-9096-1010

***Resumen*—La forma tradicional en la que se realizan las votaciones en todo ámbito en el cual se utilice este medio para la elección de lideres o representantes, es, considerando los avances tecnológicos que se tiene en la actualidad que faciliten este proceso y sobre todo que brinden una mayor confianza a los electores de los resultados de algún proceso de votación en el participen, entre las tecnologías la que más sobresale en la actualidad es la denominada Blockchain o cadena de bloques.**
**En el presente trabajo se presenta una arquitectura para el desarrollo de un sistema de votación electrónica utilizando la tecnología blockchain; en el cual se detallan los requisitos, funcionales y no funcionales, el diagrama de casos de uso obtenidos a partir de la ingeniería de requisitos y siguiendo la metodología ABCDE par el desarrollo de aplicaciones descentralizadas (DApp's).**

***Index Terms*—Blockchain, e-voting, Arquitectura, Requisitos, DApp.**

## I. Introducción

La tecnología Blockchain permite la transferencia de datos digitales con una codificación muy sofisticada y de una manera completamente segura, esta transferencia o procedimiento no requiere de un intermediario centralizado que identifique y certifique la información allí contenida, sino que se encuentra distribuida en múltiples nodos independientes entre sí, que la registran y la validan. Una vez la información se encuentra en la blockchain, "la información no puede ser borrada, solo se podrán añadir nuevos registros, y no será legitimada a menos que la mayoría de ellos se pongan de acuerdo para hacerlo" [13].

### *I-A. Características de Blockchain*

Entre las principales características, según [7], de esta tecnología tenemos:

- Descentralización
- Transparencia
- Autonomía
- Inmutabilidad
- Anonimato
- Trazabilidad

### *I-B. Tipos de Blockchain*

La tecnología Blockchain puede ser dividida en dos tipos:

- **Blockchain Pública:** es aquella que no tiene restricciones en cuanto a la lectura de sus datos y a la visualización de las transacciones para su inclusión en la blockchain, todos los participantes tienen derecho a enviar transacciones para ser validadas y posteriormente incluidas en la blockchain. Para el proceso de consenso todos los nodos tienen la posibilidad de participar [10].
- **Blockchain Privada:** es aquella que tiene acceso directo a los datos de la blockchain, pero la vista de las transacciones es limitada a una lista predefinida de entidades el permiso de escritura es mantenido por solo una organización y los permisos de lectura pueden ser públicos o, en cierta manera, restringidos arbitrariamente [10].

### *I-C. Contratos Inteligentes*

Son programas informáticos que ejecutan autónoma y automáticamente los términos de un contrato, el programa puede definir las reglas y las consecuencias estrictas del mismo, de la misma manera que lo haría un contrato tradicional, pero a diferencia de un documento legal tradicional también puede obtener información como entrada y procesarla según las reglas establecidas en el contrato para, a continuación, adoptar las medidas que se requieran como consecuencia de ello. Todo esto sin la intervención humana en el proceso [13]. Las principales características de los contratos inteligentes, según [1]:

- Inmutabilidad
- Distribución
- Deterministas
- Verificables

### *I-D. Hyperledger Fabric*

Hyperledger es una comunidad de código abierto centrada en desarrollar un conjunto de marcos, herramientas y bibliotecas estables para implementaciones de blockchain de nivel empresarial [12].
Hyperledger Fabric es uno de los proyectos mas conocidos de Hyperledger, es una infraestructura Blockchain flexible; en otras palabras, es una Blockchain privada orientada al uso empresarial, está diseñada para ser la base del desarrollo de aplicaciones empresariales, permite la creación de contratos inteligentes, llamados chaincode, que pueden ser escritos en cualquier lenguaje, pues en recientes versiones se ha integrado

el soporte para NodeJS, Java, JavaScript, etc. [9], [11], [12]. Entre las ventajas de este proyecto:

- Red con permisos
- Transacciones confidenciales
- Arquitectura conectable
- Inicio sencillo

### *I-E. e-voting*

El termino e-voting hace referencia a la votación electrónica y hace alusión a la opción de utilizar medios electrónicos para votar en los referendos y las elecciones. Un sistema de e-voting según [5], debe considerar los siguientes requisitos:

- Asegurar que solo las personas con derecho a voto están en condiciones de votar.
- Garantizar que cada voto sea contado y que sea contado una vez.
- Mantener el derecho del elector a formar y expresar su opinión de una manera libre, sin ningún tipo de coacción o influencia indebida.
- Proteger la secrecía del voto en todas las fases del proceso de votación.
- Garantizar la accesibilidad al mayor número posible de votantes, especialmente a las personas con discapacidad.
- Aumentar la confianza de los electores al maximizar la transparencia de la información sobre el funcionamiento de cada sistema.

### *I-F. Aplicación Descentralizada (DApp)*

Una DApp es una aplicación que en su mayoría o completamente esta descentralizada.
Las DApps según [8], deben cumplir con las siguientes tres características:

- **Código abierto**
  - Debe funcionar como una aplicación independiente.
  - Ninguna organización puede reclamar la posesión de la mayor parte de sus tokens.
  - Un DApp puede adaptar su protocolo en respuesta a las mejoras sugeridas y los comentarios del mercado, pero todos los cambios deben ser adoptados por consenso de todos sus usuarios.
- **Encriptación:** los datos de DApp y los informes operativos deben encriptarse y almacenarse en un dominio público, el llamado blockchain descentralizado, para evitar cualquier posible interrupción de la red.
- **Token:** una DApp debe requerir un token criptográfico (bitcoin o token de la aplicación original) para acceder a él. Cada aportación aportada por los mineros debe ser recompensada en los tokens de DApp.

### *I-G. Agile Blockchain DApp Engineering (ABCDE)*

De acuerdo a [6], ABCDE es una metodología de desarrollo de software ágil, lo que significa que sigue los principios del Manifiesto Agile. Sin embargo, se complementa el proceso ágil con un enfoque más formal, utilizando diagramas UML con una notación específica para contratos inteligentes y una lista de verificación específica para la evaluación de seguridad. Es un método completo que aborda el desarrollo de software blockchain. El método considera la integración de software entre los componentes de la cadena de bloques (contratos inteligentes, bibliotecas, estructuras de datos) y los componentes fuera de la cadena, como aplicaciones web o móviles, que en conjunto constituyen un sistema DApp completo.

## II. Trabajos Relacionados

Los trabajos relacionados encontrados, de acuerdo a la revisión bibliográfica, en Latinoamérica existen algunos proyectos en los cuales utilizan la tecnología Blockchain en el voto electrónico, con la finalidad de aumentar la confiabilidad en esta alternativa para el voto tradicional. A continuación, se mencionan algunos de ellos.

### *II-A. Modelo y sistema de votación electrónica aplicando la tecnología de cadena de bloques.*

En [2], presentan un modelo de votación electrónica en el cual integran aspectos del modelo tradicional, la tecnología blockchain y la infraestructura transaccional de la moneda criptográfica Bitcoin con la finalidad de implementar una votación descentralizada y anónima, asegurando la integridad de los datos ante cualquier posible dificultad que pueda surgir.

### *II-B. Desarrollo de un sistema de votación electrónica utilizando una tecnología de contabilidad distribuida para el almacenamiento seguro de la información*

De acuerdo a [4], el principal problema con los sistemas de votación electrónica que guardan la información en bases de datos centralizadas, es que son mucho más vulnerables al fraude que la votación en papel. Por tal motivo, el objetivo de este trabajo es desarrollar un sistema de votación electrónica utilizando una tecnología de contabilidad distribuida (DLT) para el almacenamiento seguro de la información. La ventaja que ofrece este tipo de tecnología es la descentralización, los puntos de la red verifican mediante mecanismos de consenso cada transacción realizada y almacenan la información estructurando los datos en una cadena de bloques haciendo uso de métodos criptográficos que garantizan su seguridad e inmutabilidad.

### *II-C. Implementación de un prototipo de una red descentralizada Blockchain para el voto electrónico en la universidad de Guayaquil*

En [3], menciona que entre las posibilidades de proyectos factibles con la implementación de la tecnología blockchain esta el voto electrónico, dado que esta tecnología permite la identidades de los votantes estén protegidas y los votos no puedan ser manipulados.

## III. Materiales y Métodos

En el presente trabajo, se utiliza un conjunto de materiales, métodos técnicas, normas y metodologías durante el desarrollo. En el cual se aplica métodos analíticos, deductivos e inductivos para generar la especificación de requisitos mediante el estándar IEEE830. Considerando que la emergencia sanitaria a causa del coronavirus (COVID-19) ha provocado una crisis

sin precedentes en todos los ámbitos, la cual ha generado múltiples retos tecnológicos para afrontarla. En consecuencia, el uso de las Tecnologías de la Información y la Comunicación (TIC) permitió llevar a cabo la experimentación de la primera fase. Los materiales se mencionan en el cuadro I que se muestra a continuación:

Cuadro I
MATERIALES USADOS

| **Software** | |
|---|---|
| **Detalle** | **Descripción** |
| Zoom | Software de videoconferencia que se utilizo para el trabajo colaborativo, revisiones y otras reuniones. |
| Drive | Servicio de almacenamiento en la nube y trabajo colaborativo. |
| Visio | Herramienta utilizada para la construcción de los diferentes diagramas, figuras o diseños. |
| Draw.io | Herramienta colaborativa utilizada para la construcción de los diferentes diagramas. |

## IV. EXPERIMENTACIÓN Y RESULTADOS

En base al objetivo de definir la arquitectura del sistema de voto electrónico usando la ingeniería de requisitos, para cumplir con este objetivo, intervinieron las fases de la 1 a la 4, de la metodología para el desarrollo de DApp's, denominada ABCDE. Las cuales se detallan a continuación.

### *IV-A. Fase 1: Objetivo del sistema*

El objetivo general del proyecto que es "Implementar un sistema de voto electrónico utilizando tecnología Blockchain que permita registrar votos y realizar el escrutinio de los mismos en el proceso de votación".

### *IV-B. Fase 2: Identificar los actores*

Para el desarrollo del sistema, se identificaron los siguientes actores:

- **Administrador:** el usuario encargado de administrar el sistema e-voting.
- **Usuario:** el usuario promedio que puede visualizar los resultados de una votación en proceso o alguna votación antigua en el sistema e-voting.
- **Votante:** el usuario que puede participar en alguna votación que se esté llevando a cabo.
- **SC-Users:** contrato inteligente en la blockchain de Hyperledger Fabric que tiene la funcionalidad de registrar y validar usuarios.
- **SC-Votes:** contrato(s) inteligente(s) en la blockchain de Hyperledger Fabric que tiene la funcionalidad de registrar y validar votos.

### *IV-C. Fase 3: Historias de usuario*

En esta fase se detallan los requisitos del sistema, tanto los funcionales como los no funcionales, siguiendo el estándar IEEE 830, y el diagrama de casos de uso.

*IV-C1. Requisitos funcionales:* En el cuadro II se presenta los requisitos funcionales del sistema e-voting basado en blockchain.

Cuadro II
REQUISITOS FUNCIONALES

| **Código** | **Requisito** | **Descripción** | **Prioridad** |
|---|---|---|---|
| RF01 | Iniciar Sesión | Para poder hacer uso del sistema, el administrador y el votante deben iniciar sesión con usuario y contraseña, además se debe validar si el usuario que está tratando de ingresar es un usuario que está registrado en la Blockchain. | ALTA |
| RF02 | Gestión de Votantes | El administrador puede crear partidos, actualizar sus datos y ver el listado. Además, puede agregar candidatos a estos partidos; los candidatos pueden ser cualquier votante registrado. Los partidos pertenecen a un periodo de elecciones específico. | ALTA |
| RF03 | Gestión de Partidos | El administrador puede crear partidos, actualizar sus datos y ver el listado. Además, puede agregar candidatos a estos partidos; los candidatos pueden ser cualquier votante registrado. Los partidos pertenecen a un periodo de elecciones específico. | ALTA |
| RF04 | Gestión de Elecciones | El administrador puede crear elecciones, editar sus datos y ver el listado de elecciones registradas y añadir el listado de votantes habilitados para esta elección. | ALTA |
| RF05 | Consulta de Resultados | Cualquier usuario con o sin cuenta dentro del sistema puede visualizar los resultados de las elecciones, en curso o las pasadas. | ALTA |
| RF06 | Realizar voto | El votante debe tener su sesión abierta para poder visualizar las elecciones a las que tiene permitido sufragar, dentro de cada elección podrá visualizar los partidos y sus candidatos más la opción de otorgar su voto a uno de ellos. al registrar el voto se debe confirmar la decisión, con esto el sistema registra la elección del votante al partido y envía este dato a registrar en la Blockchain. | ALTA |

*IV-C2. Requisitos no funcionales:* En el cuadro III se presentan los requisitos no funcionales del sistema e-voting basado en blockchain.

*IV-C3. Casos de uso:* En la Figura 1se muestra los diferentes actores con su respectivo caso de uso.

### *IV-D. Fase 4: Dividir el sistema en dos subsistemas*

El sistema de e-voting se procede a dividir de la siguiente manera:

- Subsistema de los contratos inteligentes que se ejecutan en la blockchain (aquí intervienen: Fase 5: Diseño del subsistema de contratos inteligentes y Fase 6: Codificación y prueba del subsistema de contratos inteligentes de la metodología ABCDE).
- Subsistema de aplicaciones, que es el sistema externo que interactúa con la blockchain (aquí intervienen: Fase 7: Diseño del subsistema de integración externa y Fase

Cuadro III
REQUISITOS NO FUNCIONALES

| Código | Requisito | Descripción | Prioridad |
|---|---|---|---|
| RNF01 | Rendimiento | El sistema debe proporcionar un tiempo de respuesta aceptable aproximadamente entre 2 a 7 segundos. La transacción tarda de 2 a 5 segundos en un ambiente simulado de red blockchain y de 15 a 5 minutos en un ambiente real. | ALTA |
| RNF02 | Usabilidad | El sistema de software debe proporcionar una interfaz amigable e intuitiva, haciendo que el proceso sea comprensible y fácil de llevar a cabo. Además, debe permitir ser utilizado en cualquier navegador web. | ALTA |
| RNF03 | Fiabilidad | El sistema de software debe permitir la disponibilidad las 24 horas del día y los 7 días de la semana, y en caso de que el módulo de software presente algún error, se debe recuperar en el menor tiempo posible. El sistema de software debe permitir recuperar los datos que se vean afectados en el caso de alguna falla en el módulo de software respecto al tiempo y esfuerzo que este genere. | ALTA |
| RNF04 | Seguridad | El sistema de software debe garantizar disminuir las vulnerabilidades de ataques de fuerza bruta. Garantizar la seguridad del módulo de software con respecto a la información y datos que se manejan tales sean documentos o archivos. | ALTA |

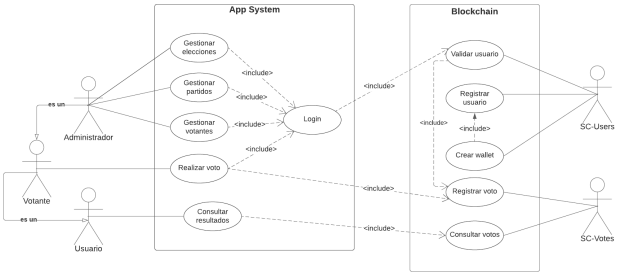


Figura 1. Diagrama de casos de uso.

8: Codificación y prueba del sistema de aplicaciones de la metodología ABCDE).

En base a estos dos subsistemas, se procede a determina el diagrama de arquitectura del software, que se detallan en la figura 2.

En la arquitectura propuesta, se hace uso de un middelware (desarrollado con Nodejs y MongoDB), dado que,a la fecha de la elaboración del proyecto, no existe forma de poder realizar la comunicación directa entre el cliente Fluter, utilizado para el desarrollo de la interfaz gráfica del cliente, y la red Hyperedger Fabric (utilizado para la elaboración de la red blockchain).

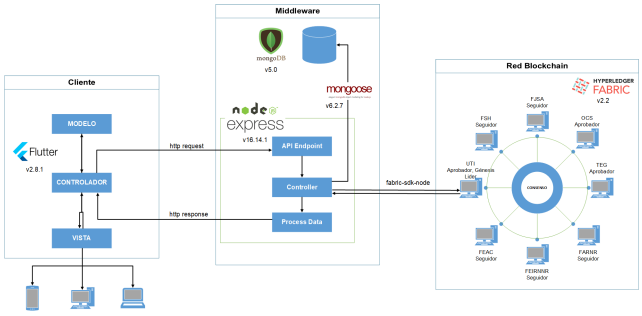


Figura 2. Arquitectura de software para el sistema de voto electrónico.

## V. CONCLUSIÓN Y TRABAJOS FUTUROS

De acuerdo a los resultados obtenidos, se concluye que seguir la metodología de desarrollo de aplicaciones descentralizadas ABCDE, permite elaborar de forma sencilla la arquitectura del sistema, al separar la parte de contratos inteligentes y la aplicación externa, esto conlleva a obtener una arquitectura más refinada de cada parte, para su posterior integración. La importancia del diagrama de arquitectura radica en que facilita la comprensión de como interactúan cada uno de los subsistemas y como se da el flujo de comunicación entre estos. Como trabajos futuros, dado que el proyecto posee un gran margen de escalabilidad, se recomienda iniciar por realizar la comunicación directa entre el cliente (Flutter) y la red blockchain (Hyperledger Fabric).

## REFERENCIAS


[1] ¿qué es hyperledger fabric? - españa — ibm.

[2] Lucuy Gabriel Alejandro, Köller Vargas Sergio, and Galaburd Yanina. Modelo y sistema de votación electrónica aplicando la tecnología de cadena de bloques. model and electronic voting system applying blockchain technology, 6 2019.

[3] VALERIA MISHELL BALDEÓN CORONEL and JOEL FRANCISCO ZAMBRANO HIDALGO. Universidad de guayaquil facultad de ciencias matemÁticas y fÍsicas, 2018.

[4] GABRIELA LISSETH ASTUDILLO CRUZ. Desarrollo de un sistema de votaciÓn electrÓnica utilizando una tecnologÍa de contabilidad distribuida para el almacenamiento seguro de la informaciÓn, 4 2021.

[5] Red de Conocimientos Electorales. Voto electrónico (e-voting).

[6] Lodovica Marchesi, Michele Marchesi, and Roberto Tonelli. Abcde—agile block chain dapp engineering. *Blockchain: Research and Applications*, 1:100002, 12 2020.

[7] Steve Moscoso, David Suárez, and Daniela Martin. Certificación digital de documentos académicos usando blockchain formato ieee. *Tecnología Investigación y Academia*, 7:21–27, 1 2020.

[8] Blockchain Academy México. Blockchain 2.0 — smart contract — daapp, 2020.

[9] Christian Peters. Building rich internet applications with node.js and express.js. *Rich Internet Applications w/HTML and Javascript*, pages 15–20, 6 2017.

[10] David Plaza. Diseño y desarrollo de diplomas académicos digitales mediante la tecnología blockchain, 2 2019.

[11] Yadu Rajiv. *Developing Turn-Based Multiplayer Games*. Apress, 2018.

[12] Krishna Rungta. Learn nodejs in 1 day, 2016.

[13] Juan Valencia. Contrato inteligentes. *Revista de Investigación en Tecnologías de la Información*, 7:1–10, 12 2019.