# Informe Blockchain

El Blockchain se ha constituido como un elemento que ha ido ganando legitimidad, de la mano con el desarrollo de la internet, como método del intercambio humano. A pesar de los grandes avances que ha tenido esta tecnología durante los últimos años, temas centrales de su escalabilidad, seguridad y sostenibilidad han tomado parte central en el debate. Según Deloitte el Blockchain es un avance tecnológico basado en conjuntos de registros que se encuentran distribuidos por cadenas de bloques (Piscini, E; Dalton, D; Kehoe, L, s.f, p. 3). Si bien, en la actualidad, el principal campo de aplicación del blockchain se ha desarrollado en el ámbito financiero: campos como: la salud, acceso a trámites públicos y servicios pueden ser ampliamente revolucionados por esta tecnología.

La aplicación de la tecnología informática en distintos campos tuvo que pasar un camino de popularización y legitimación social, esto ya que todos los temas relacionados con la red son sumamente recientes, lo cual ha significado que todos los cambios y los nuevos desarrollos sucedan en cortos periodos de tiempo. El Blockchain ha diversificado el uso de la red en “temas de la vida diaria por sus características que favorecen la resistencia a las interrupciones, auditoría y eficiencia en el transporte de datos” (Piscini, E; Dalton, D; Kehoe, L, s.f, p. 3).

Las distintas dinámicas que han existido en torno a la internet han ido generando procesos de dependencia entre el hombre y el desarrollo científico, lo cual ha requerido que modelos nuevos y clásicos se vaya acoplando a esta dinámica modernizadora. El abrupto desarrollo de las tecnologías ha avanzado de manera notable; sin embargo, esto igualmente ha generado que las vulnerabilidades se hagan cada vez más presentes y pongan en riesgo a esta dinámica. En la actualidad el negocio de la generación, el tráfico y el almacenamiento de información se ha constituido como uno de los más rentables, motivo por el cual todo el proceso cada vez requiere de la participación de actores cada vez más directos y transparentes.

La red se ha constituido como el avance tecnológico más notable de nuestra generación: por lo tanto, cuestiones básicas como el paradero de los datos generados,

seguridad, confidencialidad y trazabilidad han tenido que ser solventados sobre la marcha. Los principios que caracterizan a la red han garantizado que la producción, acceso, libertad, desarrollo, privacidad, participación y obligación se conviertan en pilares fundamentales de la internet, los cuales han acompañado gran cantidad de los procesos desarrollados. Sin embargo, se debe tener en cuenta que estos, por su popularización, han impuesto estándares requeridos por la audiencia generalizada en la red. (Internet Rights and Principles Coalition, 2011)

Las dinámicas sensibles que se desarrollan en la red deben de garantizar que solamente las partes que interactúan en una transacción puedan acceder y compartir sus datos de manera segura. Por lo tanto, el desarrollo del blockchain y su característica distributiva de los datos ha trabajado, principalmente, en su capacidad de defensa en contra de los ciberataques. A pesar de esto el blockchain no deja de ser un avance tecnológico perfectible.

El Blockchain, como se mencionó anteriormente, se ha desarrollado en varios campos, siendo el financiero su principal línea de desarrollo; no obstante, los nuevos requerimientos han generado ventanas de oportunidad para su utilización en nuevos escenarios, esto cuando la privacidad y la protección de la data una necesidad prioritaria. El presente documento analizará la factibilidad del uso del Blockchain en el ámbito electoral, para lo cual expandirá las siguientes consideraciones.

## 1.1 Administración de Blockchain para elecciones

La aplicación de formas alternativas de votación, vinculadas a la tecnología, ha sido una realidad que ha acompañado el desarrollo de la democracia en los Estados; sin embargo, las dificultades institucionales de los países han ocasionado que este proceso sea más viable en casos concretos, esto sumado a que su aplicación requiere de períodos de planificación y socialización sumamente largos. Según García-Font y Rifa-Pous “la ventana de oportunidad para la visibilización de la utilidad de la tecnología Blockchain se presentó con la entrada de las criptomonedas al mercado financiero internacional. Esto por cuanto dicho avance tecnológico

descentralizado presentó un escenario en el que el flujo de datos y la protección de los usuarios se volvió viable y normalizado" (2018, p.257).

La utilización del Blockchain en lo electoral se ha dado por dos mecanismos ampliamente diferenciados: el primero por la adquisición de tokens criptográficos para la identificación de los votantes y la segunda mediante la creación de registros de votantes inmutables que se distribuirán en las cadenas de datos. Esto ha caracterizado la aplicación de esta tecnología en ámbitos más allá de los tradicionales (financieros y de servicios), para fortalecer y promocionar el ejercicio democrático de los Estados.

La aplicación de la tecnología en "lo electoral" ha sido una iniciativa que ha generado notable de resistencia en varias naciones del mundo. A nivel contextual se debe mencionar que el aprovechamiento de la tecnología en los procesos electorales de las naciones no ha sido una búsqueda reciente, al contrario

> "el Direct Recording Electronic (DRE), aplicado en las elecciones de los Estados Unidos, se configuró como una de las primeras plataformas de voto electrónico existentes; no obstante, esta presentó problemas de bugs y alta vulnerabilidad a agresiones externas en el ámbito digital digital" (García, V; Rifa, H, 2018, p. 258).

Dichas vulnerabilidades alimentaron las dudas al respecto de su aplicación, qué decir de procesos que requieran aún más de la utilización de la red, lo cual dificulte la aplicación progresiva de estos modelos en países con limitaciones tecnológicas.

A nivel práctico la utilización de la tecnología en los procesos electorales sugiere un mecanismo para la resolución de problemas relacionados con la ejecución del derecho al voto, las cuales van desde la captación y procesamiento de votos en el extranjero, el voto preferente (voto en casa), la prevención de la aglomeración de personas en los recintos electorales y el procesamiento de datos en tiempo real. El uso de la tecnología en los procesos electorales, como se había mencionado, no es algo reciente, en la actualidad gran parte de los procesos electorales "tradicionales" que se llevan al cabo de manera presencial en boletas de papel, requieren de un proceso de digitalización y de transmisión de datos para conteo y

procesamiento de resultados, más cuando la presentación de resultados y el conteo rápido son mecanismos legitimadores de la democracia y de los procesos electorales “per se”.

Según García y Rifa los procesos de votación electrónica buscan legitimar una serie de procesos necesarios para el desarrollo de la democracia, los cuales son:

**Elegibilidad:** Esto ya que solo son los votantes que se encuentran debidamente registrados pueden participar en el proceso.

**Autenticidad:** En respeto a la idea de que cada votante representa un solo voto, el cual debe ser respetado en todos los instantes de la votación.

**Privacidad:** Misma que es una necesidad de todo proceso electoral, tanto físico como digital, en la que la trazabilidad o identificación del votante no sea una opción que se realice de manera secreta.

**Secreto de los resultados Intermedios:** Si bien la presentación de resultados rápidos es una práctica que ha legitimado el normal trajín de los procesos electorales, es necesario mencionar que todo mecanismo de presentación temprana de los resultados requiere de la planificación de cada organismo electoral. Por lo tanto, ningún proceso de seguimiento puede ser presentado por fuera del cronograma establecido.

**Incoercibilidad:** Los sistemas y la propia ejecución del derecho al voto, no pueden permitir que el votante sea víctima de coerción por parte de las autoridades o las personas interesadas en el resultado de un proceso electoral.

**Verificabilidad E2E (extremo a extremo):** Es necesario que las partes que se encuentran inmiscuidas en un proceso sean capaces de verificar el desarrollo del proceso electoral. Es decir, los votantes pueden verificar el registro de su voto, mientras que la organización político pude comprobar el proceso de escrutinio y procesamiento de los datos desde el depósito en la urna de votación virtual.

Los procesos de aplicación de una votación digital requieren de la utilización de varios servicios. Para la buena ejecución de un proceso electoral, es necesario mencionar que, la

implementación de un sistema no hostil que permita al votante la selección de la opción de su preferencia, es una necesidad por parte del proveedor del servicio. Por su parte, la filtración de los votos duplicados y aquellos que no se consideran consistentes es un requerimiento del proceso electoral que se encuentra en las competencias del órgano rector de una elección.

El mezclado de votos para eliminar su trazabilidad es una necesidad imperante de todo proceso de votación electrónica. Esto ya que el registro de entrada del votante y el momento del depósito del voto no pueden ser vinculado a ninguna persona. De igual manera, el seguimiento del proceso por parte de todos los actores involucrados en una elección legitima y sostiene la credibilidad social en el proceso.

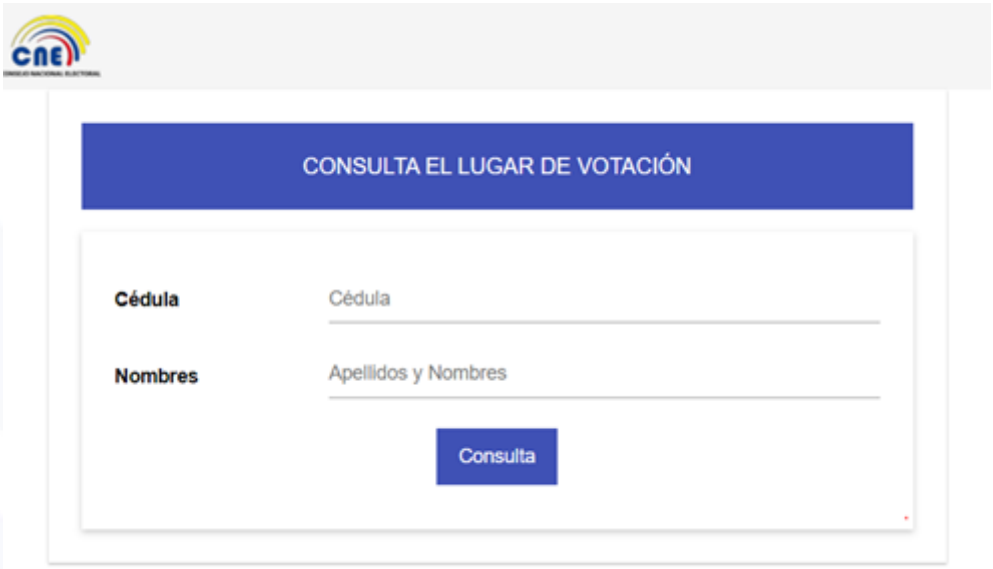
**¿De qué manera se realizaría la autentificación de la persona que está votando?**

El artículo 12 de la Ley Reformatoria a la Ley Orgánica Electoral y de organizaciones políticas indica: *La calidad de electora a elector se probará por la constancia de su nombre en el registro electoral. La verificación será efectuada en la correspondiente junta receptora del voto con la presentación de la cédula de identidad, el pasaporte, o el documento de identidad consular. La no vigencia de estos documentos no impedirá el ejercicio del derecho al sufragio."*

Actualmente contamos con la información que guarda la nueva cédula, la cual nos puede servir para validar que es efectivamente el votante quien está ejerciendo su derecho al voto. Esta información se almacena como:

Con el número de cédula, el código dactilar y algún otro parámetro de comprobación de identidad (mostrados anteriormente), podemos acceder a un portal como el que existe actualmente para consultar el recinto electoral (como se muestra en la siguiente figura).


Este portal luego de validar al votante puede generar un link único que expire después de determinado tiempo o una contraseña única con tiempo de expiración para que las personas ingresen a un aplicativo. Este podría satisfacer las siguientes necesidades:




· De consulta, ya que mediante el diseño de un formulario se puede captar la voluntad del ciudadano a ejercer la votación electrónica.

· De cambio de domicilio electoral, a través de una herramienta que permita al ciudadano guardar su ubicación o ingresar su dirección.

· De sufragio, a partir de un aplicativo o portal en el cual se encuentren electrónicamente las papeletas, de tal forma que puedan los votantes elegir algún candidato, anular o dejar en blanco; para finalmente guardar su proceso mismo que puede generar electrónicamente un certificado de votación válido para ser impreso o usado como certificado digital.

· De monitoreo, para facilitar el conteo rápido y la detención de eventos anómalos.

Este módulo de Seguridad dentro de la plataforma debe estar atado a un Firewall de la base de datos o padrón electoral que protege y encripta la información y a su vez esta atado a un factor de autenticación múltiple con:

**Preguntas de seguridad**

Para reforzar la seguridad de que el votante sea realmente el que accede a estos servicios, se puede hacer consulta a las bases de datos abiertos (i.e. IESS, ANT, SRI, Registro Civil, etc.) usando su número de cédula, de tal forma que se puedan plantear preguntas de seguridad robustas.

Este módulo de autenticación a su vez debe estar atado a un módulo de auditoría para que se pueda verificar en cada fase que se hizo sea el administrador o un digitador incluyendo un **DLP Data Lost Prevention** que incluye una bitácora o registro de lo que cada usuario realizó.

Como se ha mencionado anteriormente el Blockchain posee características ampliamente aplicables a los procesos electorales. Las distintas elecciones que se han realizado de la mano con esta tecnología la han utilizado ya sea en una sola de sus instancias o para sustentar la ejecución entera de esta. Durante el presente trabajo hemos definido que la utilización del Blockchain en procesos electorales podía realizarse de dos maneras, por medio de la utilización de tokens criptográficos o por la creación de bancos de votantes distribuidos a

lo largo de una cadena de registros, lo cual nos permite diferenciar el mecanismo de análisis de cada una de estas posibilidades.

El modelo Blockchain que ha sido trasladado desde las criptomonedas hacia lo electoral, ha pensando que cada una de las personas empadronadas en un proceso electoral corresponde a una cantidad (unidad) de moneda electrónica. Esto permite trasladar desde el sistema financiero las experiencias obtenidos para la protección de los usuarios y el entendimiento de cada voto como una dirección (similar a una cuenta bancaria).

El gráfico número 1 nos permite entender cómo el vínculo entre las transacciones de criptomonedas y los sistemas electorales puede ser realizadas. Este proceso requiere de las siguientes consideraciones.

1. El organismo electoral, que funciona como administrador del proceso, habilita a cada votante registrado con una unidad de valor que en este caso corresponde un voto. Esta unidad es utilizable solo en una ocasión y se configura como la voluntad de cada persona en un proceso electoral. En este escenario el organismo electoral es un elemento fundamental para el proceso de empadronamiento y administración de las unidades de valor a cada votante.

2. En el segundo punto los votantes son habilitados con una unidad de valor, la cual se codifica y se vincula a cada individuo, esto sin la voluntad de rastrear al usuario ni la manera en la que este ejerce su voto. Al contrario, esto permite que cada entrega de una unidad de voto no pueda ser modificada y pueda generar inconsistencias electorales. Es decir este proceso permitirá saber el cumplimiento del derecho al voto; pero, permitiendo que su vínculo se pierda una vez realizado. Tras esto el reordenamiento del voto de cada persona se almacena y se dirige hacia las cuentas asignadas a cada candidato.

3. El tercer paso para realización del proceso electoral es la asignación de cada una de las unidades de voto a las cuentas codificadas de cada uno de los candidatos participantes en la contienda. Se debe decir que estos votos en este punto ya no se encuentran

vinculados a una persona en específico, al contrario se registran como votos depositados sin anomalías en el recinto electoral designado.

4. Una vez que la votación termina el organismo electoral y las distintas empresas intermedias que ayudan a los procesos de división de datos y fiscalización del proceso, revisan los resultados y determinan la normalidad de todas las transacciones realizadas durante el proceso. Esto requiere de una aplicación logarítmica que filtre movimientos sospechosos que permitan auditar de mejor manera las inconsistencias que puedan presentarse.

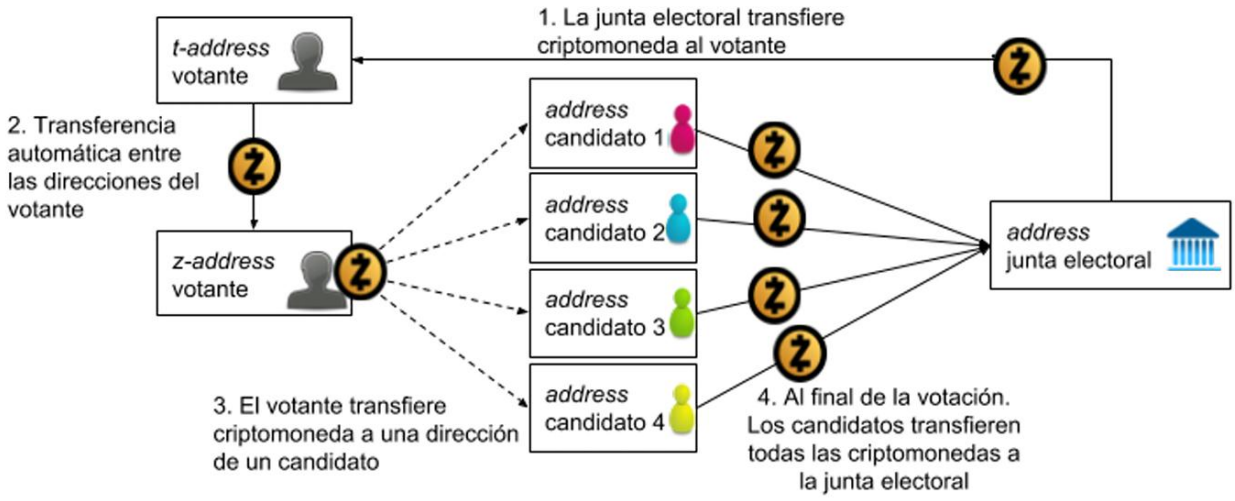



Gráfico 1: Sistemas electorales y modelos de criptomonedas. Tomado de Tarasov y Tewari, 2017

La división de los datos en la red creada para el encadenamiento de los datos puede tener varias formas. Según Lucuy, Koller, Galaburda "La administración y el almacenamiento de datos depende el número de nodos inmiscuidos en el almacenamiento. Las redes centralizadas por un solo nodo dividen la data en un administrador central, mientras que en

los sistemas distribuidos, todas las partes involucradas tienen acceso y una copia de toda la información' (Lucuy, G; Koller, S; Galaburda, Y, 2019, p. 239).

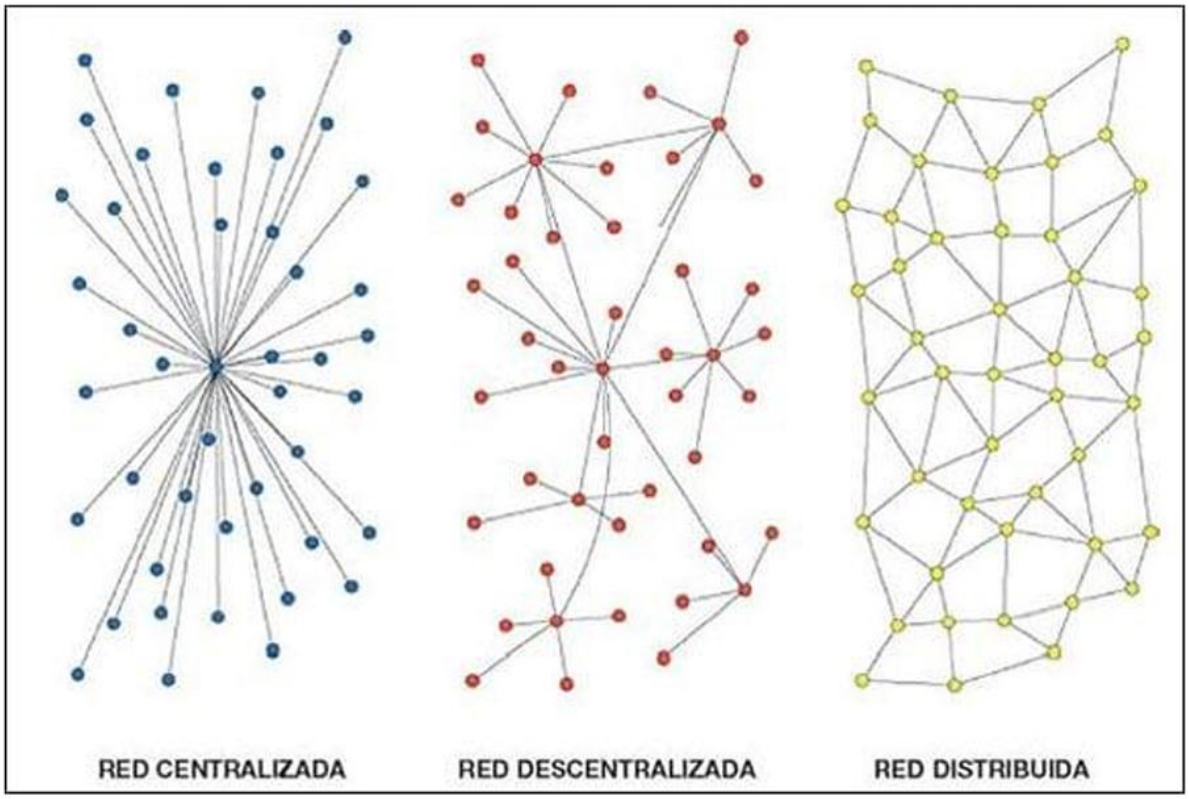



Gráfico 2: Tipo de redes. Tomado de Lucuy, G; Koller, S; Galaburda, Y. 2019

La distribución de los nodos de un sistema Blockchain se puede dar de tres maneras diferentes. En primer lugar, el Blockchain público que es aquel que se vincula a las criptomonedas y las hace accesibles para cualquier individuo con una conexión a internet, este proceso es abierto al público y todo usuario del sistema tiene posibilidad de ver el estado actual de las transacciones existentes. En segundo lugar, el Blockchain Privado en el acceso solamente se ha factible cuando se concede un acceso por parte del administrador del sistema, las principales acciones del sistema solamente pueden ser realizadas por ciertos nodos con permisos especiales. Por último, el Blockchain híbrido es una combinación de los métodos antes mencionados, esto gracias a la aplicación de permisos hacia ciertos nodos del

sistema y a la transparencia en cuanto al seguimiento a tiempo real por parte de los usuarios con una conexión a internet (Lucuy, G; Koller, S; Galaburda, Y. 2019, p. 240).

Todo sistema de Blockchain, indiferentemente de su tipo, requiere del trabajo conjunto entre los sistemas informáticos y las personas que los administran, si bien el presente trabajo plantea una aproximación a un sistema electoral conducido por blockchain. El gráfico número 3 ejemplifica los distintos actores que se encuentran involucrados en la administración y el flujo de datos del sistema, este requiere de la presencia humana en cada uno de las distintas instancias del proceso, lo cual hace indispensable la presencia de administradores físicos en el proceso.

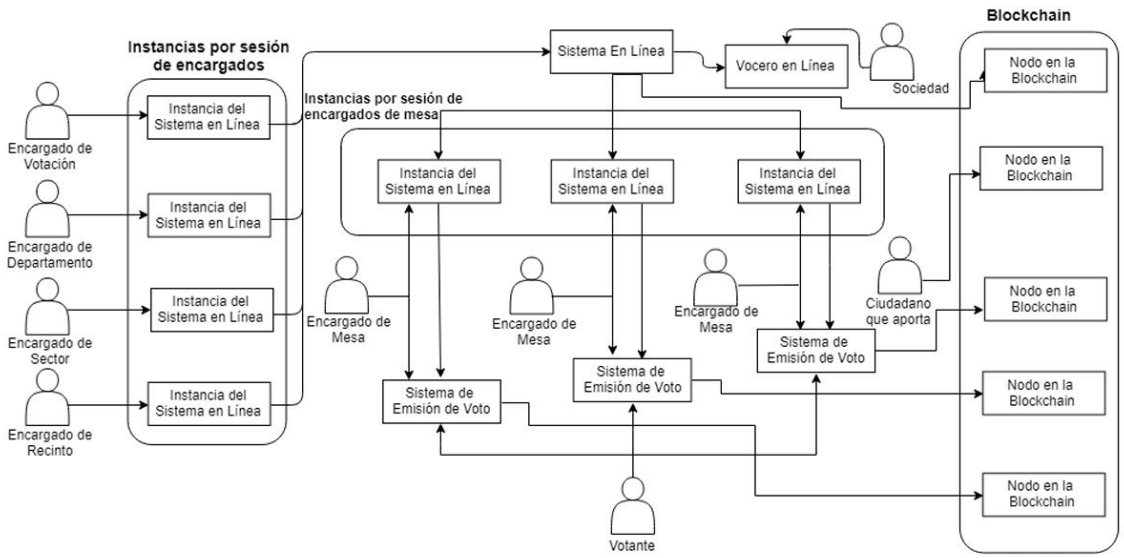



Gráfico 3: Relación entre actores y un modelo electoral por Blockchain. Tomado de Lucuy, G; Koller, S; Galaburda, Y. 2019

**¿Cómo se realizan las auditorías técnicas al blockchain?**

Los procesos de auditoría posibles durante los procesos electorales llevados con blockchain, se eslabonan con cuestiones propias de los distintos estadíos de estas. Es necesario mencionar que todo proceso electoral digital necesita de administradores que examinen las distintas secciones de la cadena de transmisión y almacenamiento de datos. Los exámenes de auditoría de una elección llevada mediante el proceso Blockchain se producen al dividir la votación de la autenticación del ciudadano.

Si bien el periodo previo al momento de la votación requiere de la asignación de los identificativos a los ciudadanos habilitados para ejercer su derecho al voto -proceso encabezado por la función electoral- dicho seguimiento se suspende al momento en el que el ciudadano ejerce su voto y este entra a la urna virtual y al sistema de asignación del unidades de voto a los distintos candidatos. Los procesos de revisión de los votos pueden ocurrir en el momento de la codificación de los usuarios, durante el mezclado de votos en la urna virtual que evita la trazabilidad o en el proceso de asignación de votos a cada usuario. Esto permite que se pueda elaborar la auditoría sin violar el secreto al voto.

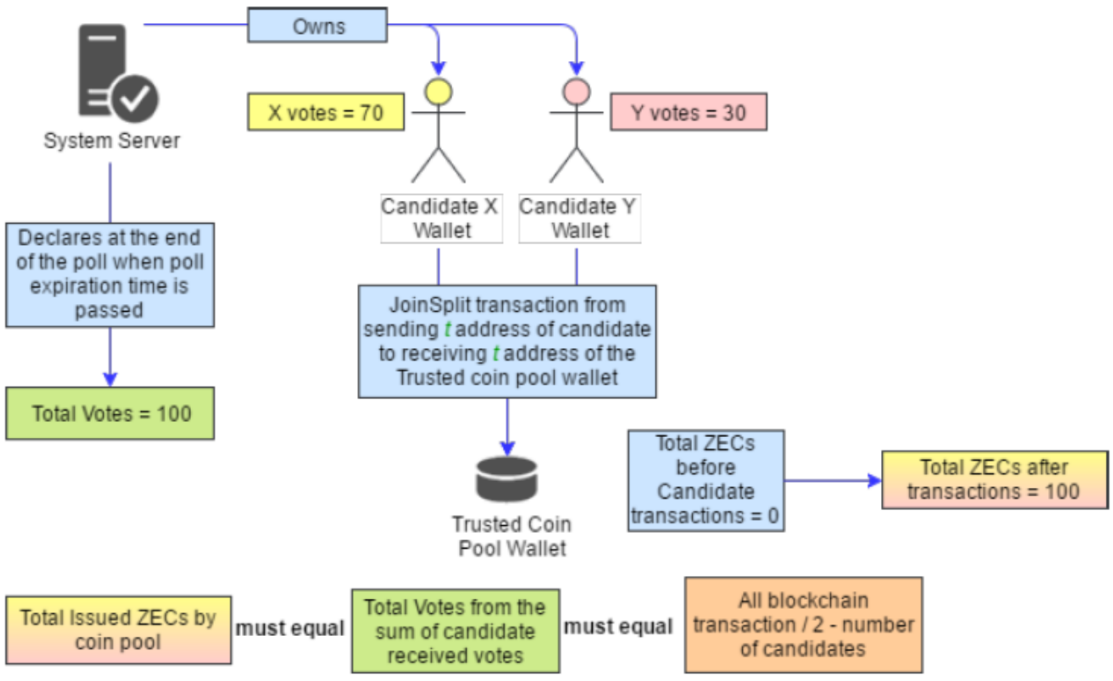


Gráfico 4: Ejemplo de auditoria electrónica a un proceso electoral llevado mediante Blockchain. Tomado de Tarasovy, P; Tewari, H, 2017.

**¿Cómo se puede aplicar el blockchain para el escrutinio público?**

El escrutinio público Si hablamos en específico del voto telemático (o voto por internet u on-line), la legislación ecuatoriana[1] en su capítulo octavo, votación y escrutinio, sección segunda, votación electrónica, artículo 51 que sustituyó el Art. 113, menciona que:

*"Art. 113.- El Consejo Nacional Electoral podrá decidir la utilización de métodos electrónicos o telemáticos de votación y escrutinio en forma total o parcial, para las diferentes elecciones previstas en esta Ley. En este caso introducirá modificaciones a su normativa de acuerdo al desarrollo de la tecnología.*

*A fin de promover y garantizar la mayor participación electoral de las personas ecuatorianas en el exterior, el Consejo Nacional Electoral, priorizará el empleo de métodos electrónicos o telemáticos de votación garantizando las seguridades y facilidades suficientes. Así mismo, podrá facilitar el voto anticipado por correspondencia, de conformidad con la normativa que dicte para el efecto y que garantice que el voto sea secreto y escrutado públicamente" (Constitución de la Republica del Ecuador, 2008()*

Es decir que, en la actualidad las elecciones tienen al menos dos requisitos usuales tanto en la votación presencial como electrónica. Estos requisitos son:

1. **Anonimidad (sigilo del voto)**. - No debe haber forma de que alguien más sepa por quién votamos, ni si siquiera durante el conteo de votos o después. De esta forma, nadie puede ser expuesto a sobornos o amenazas para votar de una forma u otra.

2. **Confianza (escrutinio público). –** Es importante que el sistema asegure que los votos sean seguros y contados con precisión, pero además es importante que sea obvio para todos los actores políticos, sin importar su formación académica, que el sistema es confiable. Cuando votamos depositamos la papeleta en una urna sellada a

la que retirarán todas sus seguridades al final del proceso frente a los ojos vigilantes de los delegados por los partidos políticos, así como los del CNE. De ninguna forma esta confianza es basada en las personas si no en el sistema electoral, sus métodos y en las pruebas físicas que son los votos, tanto para declarar ganadores como para reconteos.

Asi esta base de datos debe tener un block de registro de todas las acciones que se realizan durante la jornada electoral, esta bitácora de acciones puede tener miles de formas de presentar los datos y verificar la información así se necesita que la **Junta Electoral Especial de Contingencia Sanitaria** sea conformada por expertos en ciberseguridad quienes puedan interpretar las estadísticas mediante Business Intelligence **BI** y la minería de datos permite presentar diferentes análisis en tiempo real.

Software: Un ejemplo es una aplicación desarrollada en Python con el sistema operativo Linux. Esta no guarda información relativa a la selección efectuada por electores, asegurando que no exista trazabilidad y garantizando la confidencialidad del mismo. Así también, automatiza 100% el proceso de votación, permite imprimir el recibo de voto y ofrece un registro físico y electrónico.

De hecho, Yi (2019) menciona que debido a que el voto electrónico es un tema urgente en el área de comunicaciones y que las preocupaciones en temas de seguridad informática son uno de sus principales obstáculos, existen técnicas de blockchain[2] en redes P2P [3]que pueden mejorar la seguridad del voto electrónico, con el esquema que se muestra a continuación.

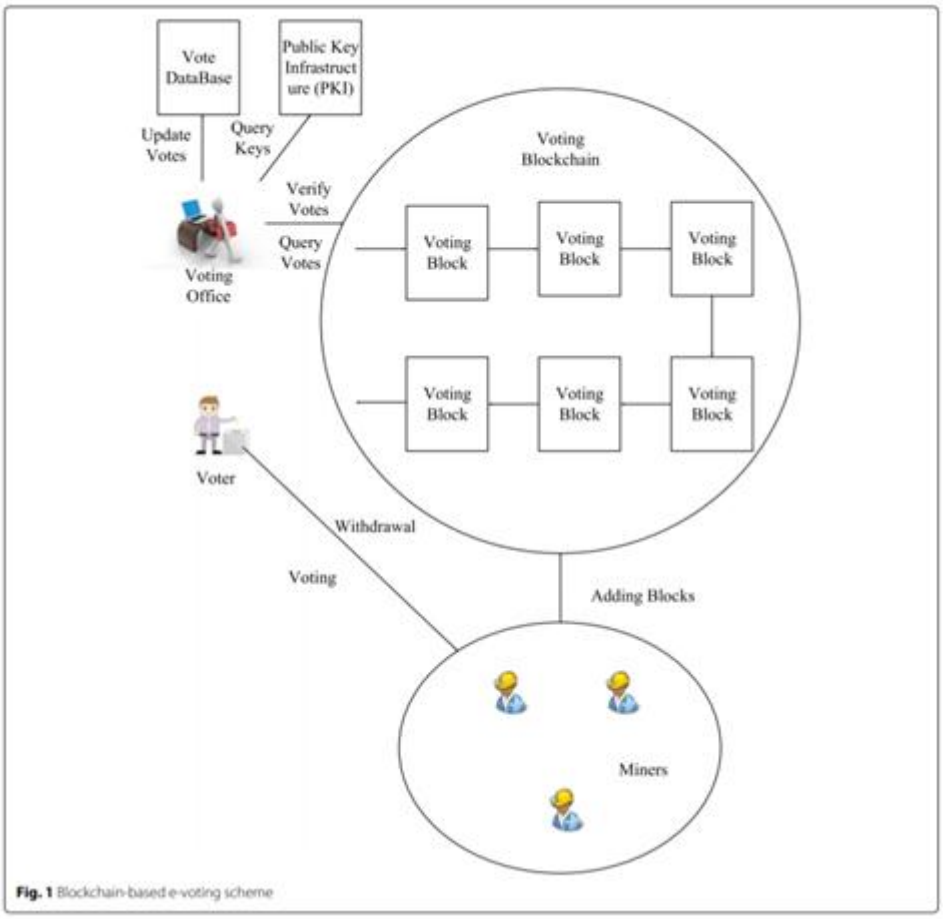


**Fig. 1** Blockchain-based e-voting scheme

En esta figura los papeles están bien definidos: votantes son quienes depositan sus votos en el dispositivo o sitio web, los mineros se encargan de agregar los votos validados a la cadena de bloques que luego ingresa a la oficina de votos donde se consultan y cuenta los votos, guardando siempre la confidencialidad del proceso.

---

[2] Una cadena de bloques o blockchain es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se les añade meta informaciones relativas a otro bloque de la cadena anterior en una línea temporal, de manera que gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser

repudiada o editada modificando todos los bloques posteriores. Esta propiedad permite su aplicación en un entorno distribuido de manera que la estructura de datos blockchain puede ejercer de base de datos pública no relacional que contenga un histórico irrefutable de información.

[3] Una red peer-to-peer, red de pares, red entre iguales o red entre pares (P2P, por sus siglas en inglés) es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí (https://es.wikipedia.org/wiki/Peer-to-peer).

---

**[1]** Ley Reformatoria a la Ley Orgánica Electoral, Código de la Democracia, Registro Oficial del 20-Febrero-2020.

**¿Cómo se puede aplicar el blockchain para el reconteo de votos?**

La tecnología blockchain ha tenido repuntes notables, Hashchain se ha configurado como una de las opciones más importantes a la hora de tratar la utilización de este sistema en los procesos electorales. Esta permite separar y mantener la privacidad del ciudadano, pero se puede permitir el acceso mediante claves encriptadas sobre las cuales se puede hacer todas las auditorías, es decir, requiere como parte fundamental de su proceso de funcionamiento la encriptación de datos.

Esta actúa desde el depósito de los votos en las urnas digitales. Al ser virtuales, esas urnas pueden ser abiertas informáticamente. Lo que se hace es separar la identificación del ciudadano con su voto. Luego esta urna se somete a un algoritmo que encripta y mezcla exclusivamente la integregrad de los votos.

El gráfico número 5 nos permite observar como un dato ingresado en el sistema empieza a encriptarse, diferenciando su origen del estadío previo durante distintas fases del proceso. La propuesta de mezclado en una urna electrónica, para evitar vinculación del votante y el voto, cuenta como el primer paso para la transmisión y el almacenamiento de los datos.

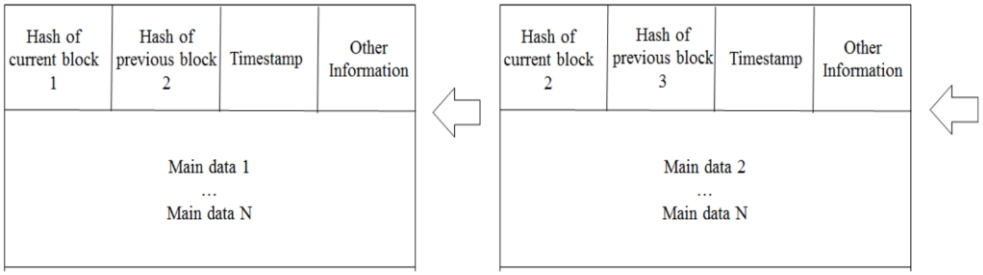



Gráfico 5: Estructura de un sistema Hashchain. Tomado de Tarasovy, P; Tewari, H. (2017)

**¿Cuáles son las seguridades que implicaría el blockchain para el voto telemático? y ¿quién administraría?**

La administración siempre va a a estar a cargo del Consejo Nacional Electoral, donde la administración será siempre del CNE. Se puede crear réplicas de esta información a otros sistemas (como otras redes académicas, y Organizaciones Políticas) que permitirá acceso y diseminación de toda la información.

El Blockchain, al igual que varios avances tecnológicos de la última década, ha generado un marcado debate en la sociedad civil. Si bien esta tecnología se ha configurado como un método disruptivo en la escena de la protección, almacenamiento y transmisión de datos, cuestiones básicas relacionadas con el paradero de los datos y el posible espionaje de las transacciones se han convertido en un factor que debe ser solucionado para la legitimación de este en el largo plazo.

En la actualidad los diferentes avances tecnológicos requieren de un proceso de puesta a punto que permitan ser utilizados en diferentes campos. El Blockchain inició como un requerimiento de los usuarios para ¨recobrar el control de sus operaciones y acciones,

generando inestabilidad en los estándares actuales basados en la centralización y verificación por parte de terceras partes¨ (Cano, J, 2018, p. 46). El Blockchain en la actualidad no solamente debe generar buenos resultados en los diferentes campos en los cuales se ha desarrollado, al contrario debe generar un sistema de confianza que se pueda sostener en el largo plazo.

La capacidad de descentralizar el manejo de los datos con la finalidad de minimizar el traspaso y la vulnerabilidad de un sistema, hacen sumamente interesantes a las opciones vinculadas al Blockchain. A pesar de esto, se debe decir que el debate relacionado con las partes involucradas en el proceso de almacenamiento de datos y la definición de un administrador o moderador central aún siguen generando incógnitas que solamente pueden ser solucionadas en la práctica. La presente sección busca generalizar los debates de seguridad de la mano con este sistema.

Cuando se discute a la tecnología vinculada a las cadenas de bloques, como en cualquier otro tipo de tecnología, se debe tener en cuenta que a pesar de su gran fiabilidad esta no es infalible. Esto ya que en la actualidad no se ha desarrollado una tecnología que pueda considerarse invulnerable. Según Lin y Lao existen una serie de posibles escenarios en los cuales el Blockchain puede ser vulnerable. (2017)

1. **Ataques a las Estampas de Tiempo:** Sucede cuando el atacante altera el contador de tiempo de un eslabón de la red, la cual ante esta vulnerabilidad puede aceptar datos alternativos, introducidos por el atacante, en el sistema. Esto además de alterar la fiabilidad de la información, puede afectar el uso de datos computacionales y afectar el procesos de auditoría posterior. De acuerdo con Márquez un ataque coordinado a varias partes de la cadena de bloques con una capacidad de cómputo mayor a la que esté manteniendo el proceso blockchain (en nuestro caso los servidores electorales) pueden por en riesgo la veracidad de los datos. Esto por el reemplazo de pedazos de la cantena, lo que puede presentar datos alterados. (Márquez, S, 2017)

2. **Ataques a los Hash de los bloques:** Es una vulnerabilidad que ataca el valor del hash[1] de una transacción recientemente autorizada. Este tipo de ataque puede provocar que el hash modificado llegue a un nodo de minería antes que el hash "original", lo que puede alterar el resultado final mostrado (Zheng, Z., Xie, S.,Dai, H., Chen, X. y Wang, H. 2017).

**Conclusiones:**

En conclusión, es necesario mencionar que los procesos de votación, en el marco de la emergencia sanitaria provocada por el COVID-19, han obligado a varios organismos electorales a modificar procesos democráticos planificados. Es necesario mencionar que en el caso ecuatoriano los desafios en el corto y mediano plazo son sumamente altos, esto por la necesidad de adaptar el proceso electoral planificado en el 2021 a la nueva normalidad que se nos ha presentado. El reto de trabajar de manera planificada supone un desafío fundamental para la función electoral, la cual tiene en sus manos el mantenimiento de la Democracia en un momento coyuntural sumamente complejo.

En ese sentido, tras el análisis de caso de la votación en Blockchain/Hashchain, se ha definido que cualquier escenario electoral deberá incluir al voto telemático y al voto presencial. Esto con la finalidad de atender de mejor manera las realidades, en ocasiones sumamente desiguales, presentes en el Ecuador.

[1] "Una función criptográfica hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud" (Donohue, B, 2014)

## Bibliografía

Cano,J. (2018). Blockchain: Cadena de Bloques. Reflexiones sobre seguridad y contro . XVI Jornada de Gerencia de Proyectos de TI. Club de la FAC

García-Font, V; Rifa-Pous, H. (2018). Uso y retos de blockchain en plataformas de votación electrónica. RCSE XV: Sesión. Seguridad y e-Administración

Habo, Yi. (2019). Securing e-voting based on blockchain in P2P network. EURASIP Journal on Wireless Communications and Networking

Internet Rights and Principles Coalition. (2011). Carta de Derechos Humanos y Principios en Internet.

Karpersky Daily. (2014). ¿Qué es un hash y cómo funciona?. Archivo digital recuperado el 3 de mayo de 2020 de https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

Lin, I. y Liao, T. (2017) A Survey of Blockchain Security Issues and Challenges. International Journal of Network Security. 19, 5. 653-659

Lucuy, G; Koller, S; Galaburda, Y. (2019). Modelo y sistema de votación electrónica aplicando la tecnología de cadenas de bloques. Acta Nova; n 2. p.p 236-256

Márquez, S. (2017) Seguridad y blockchain. En Preukschat, A., Kuchkovsky, C., Gómez, G., Díez, D. y Molero, I. (2017) Blockchain. La revolución industrial del internet. Barcelona, España: Gestión 2000. 227-233

Piscini, E; Dalton, D; Kehoe. L, (s.f). Deloitte: Blockchain y Ciberseguridad, Deloitte global cyber SMEs

Tarasovy, P; Tewari, H. (2017). The future of e-voting. Int Journal. on CS & I.S, vol 12, n2, pp. 148-165.

Zheng, Z., Xie, S.,Dai, H., Chen, X. y Wang, H. (2017) An Overview of Blockchain Technology:Architecture, Consensus, and Future Trends. Proceedings of 2017 IEEE 6th International Congress on Big Data. IEEE Computer Society. 557564. Doi: 10.1109/BigDataCongress.2017.85+

| |
|---|
| **Realizado**: Ismael Jaramillo, Lupe Falconí |
| **Aprobado**: María José Calderón, Phd |