Sistema de Votación online para entornos académicos, corporativos y organizacionales basado en Blockchain

Castro Cristhian[0000−0002−1470−6851], Kogan Pablo[0000−0003−1195−7556], and Lagori Rodolfo[0000−0001−7514−2685]

Facultad de Informática - Universidad Nacional del Comahue
Buenos Aires 1400, 8300 Neuquén, Argentina
cristhian.castro|pablo.kogan|rodolfo.lagori@fi.uncoma.edu.ar

Resumen En este trabajo se analiza el desarrollo de una herramienta que permita la gestión de votaciones [9], de tipo BBB-Voting (Blockchain-Based Boardroom Voting) en el Consejo Directivo de la Facultad de Informática de la Universidad Nacional del Comahue utilizando la Blockchain Federal Argentina pero sin limitarse a ella. El objetivo es el análisis técnico y pragmático de un sistema de votación online que facilite la toma de decisiones democráticas en entornos académicos, institucionales y corporativos.
Se analizará su importancia, las características que debería tener, así como posibles herramientas que sirvan para este cometido.Se plantearán diferentes alternativas para el diseño de la arquitectura elegida, permitiendo continuar este trabajo en lineas futuras.

Keywords: Sistemas de Votación · Boardroom Voting · Blockchain

1. Introducción

El surgimiento de la pandemia SARS-Covid19 a finales de 2019 y comienzos del 2020 (y aún vigente al momento de la redacción de este documento), implicó un desafío exorbitante para la humanidad, la cual, para hacer frente a esta amenaza, debió cambiar numerosos paradigmas que trascendían la totalidad de las culturas del mundo y que las atravesaban en todos los aspectos de la vida cotidiana[1].

Los ámbitos laborales y académicos no fueron exceptuados. Muchas actividades que tradicionalmente se desarrollaban en espacios determinados y debidamente acondicionados para facilitar la reunión de numerosos grupos de personas, se vieron repentinamente cerrados e inutilizados. El distanciamiento social es una de las armas más eficaces que dispone la humanidad para hacer frente a la pandemia, no obstante, la necesidad de las personas de interactuar entre sí para continuar con los procesos económicos y académicos continúa en vigencia.

[1] https://www.who.int/es/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—11-march-2020

En este sentido, los actores e involucrados en estos procesos recurrieron a la tecnología para salvar los problemas organizativos que supone la distancia física entre personas. Muchos trabajos que tradicionalmente eran realizados en oficinas, ahora pueden ser realizados, sin mayores cambios, desde los domicilios de los propios actores, y en este sentido, las plataformas que brindan un soporte para la realización de videollamadas online adquirieron un rol fundamental. Sin embargo, hay necesidades específicas dentro de los flujos de trabajo de las personas, que estas plataformas no alcanzan a cubrir, ya sea porque no está dentro del propio alcance de la herramienta, o bien porque la funcionalidad ofrecida por la misma es demasiado genérica, atenta a cubrir el máximo de casos de uso posible.

Es en este contexto en que existe la necesidad por parte de numerosas organizaciones, tanto empresariales, corporativas como académicas, sobre todo por parte de aquellos encargados de la toma de decisiones, de contar con una plataforma que permita a los participantes, asistentes o encargados de la toma de decisiones, participar de manera democrática y transparente en una elección, realizada de manera presencial, y actualmente llevada a cabo a través de internet.

Esta necesidad implica desafíos que de otra forma no hubiesen surgido. Es necesario poder garantizar que el voto emitido por una persona permanezca inalterado hasta su recuento y procesamiento, a su vez, poder garantizar la autenticidad de la persona. También es importante que la plataforma permita realizar un recuento y procesamiento de los votos acorde a las reglas de negocio que rigen el sistema electoral, y esto implica necesariamente, la gestión de casos atípicos que antes, en la era presencial, no ocurrían, tales como la interrupción de la participación de un elector por el corte de energía eléctrica o desconexión por ejemplo.

A partir del año 2015 la Facultad de Informática de la Universidad Nacional del Comahue comenzó a desarrollar una Línea de Investigación y Desarrollo articulada a iniciativas en el ámbito de la Universidad y el contexto local que proponen abordar el campo de los sistemas de votación. Dentro del ámbito de la Universidad se ha desarrollado el sistema Gukena [2] que gestiona el centro de cómputos de las Elecciones de la Universidad, logrando mejorar velocidad, comprensión y transparencia de los resultados [11]. Así mismo, se ha participado en la observación de los procesos electorales locales, aportando mejoras a los procedimientos [3] de la Justicia electoral para las elecciones de la Provincia de Neuquén en donde se utiliza el sistema de boleta única electrónica [7].

Es en este contexto, y ampliando la Línea de Investigación y Desarrollo relativa a sistemas de votación online, es que se analiza la implementación y/o despliegue de una herramienta que cubra las necesidades anteriormente planteadas. Tal herramienta está tipificada dentro de los denominados sistemas BBB-Voting (Blockchain-Based Boardroom Voting), cuya principal característica es que fue-

[2] https://resultados.uncoma.edu.ar/gukena/

[3] http://www.jusneuquen.gov.ar/eleccion-municipalidad-de-neuquen-22-de-septiembre-de-2019/

ron diseñados para entornos y comunidades relativamente chicas, tal como un Consejo Directivo, una Junta Directiva o cualquier grupo acotado de toma de decisiones en grado democrático. En este sentido, vale aclarar que este documento no propone un sistema de votación online a fin de gestionar procesos electorales generales, relacionados con la elección de autoridades en el ámbito estatal y/o público. Las razones son, por un lado, la arquitectura propuesta, como se verá mas adelante, no está dimensionada para tal caso; así mismo las reglas de negocio que rigen un sistema y el otro, son totalmente distintas; una elección general supone un dominio más complejo que no permite asegurar el secreto, la integridad y la auditabilidad del voto [3].

El documento se organiza de la siguiente manera. En la sección 2, se presentan las condiciones que debe cumplir un sistema de votación online y la forma en blockchain puede ayudar a contribuir al cumplimiento de estas condiciones. En ese sentido se presenta blockchain y en particular Blockchain Federal Argentina (BFA). En la sección 3, se presentan algunos trabajo que abarcan la misma problemática, generando distintos sistemas que deben ser analizados.

En la sección 4 se detalla la propuesta a desarrollar para la confección de un sistema ad-hoc que cumpla con las condiciones planteadas. En documento cierra con la sección 5, en la que se formulan conclusiones elaboradas en el ámbito de este desarrollo y se postulan líneas de trabajo futuro.

2. Marco Conceptual

Un sistema de votación online, a pesar de ser necesario dado el contexto actual, es también un tanto controversial en la sociedad, ya que siempre está latente el riesgo de fraude. Por esta razón, existen condiciones y requisitos que el sistema debe necesariamente cumplir para disminuir al máximo posible este riesgo y otorgarle al sistema la máxima confiabilidad posible.

2.1. Condiciones generales del e-voting

Todo sistema de votación online tiene una serie de condiciones y requerimientos que cumplir [10] [3]. Entre los de mayor importancia y de mínimo cumplimiento podemos destacar los siguientes:

- Asegurar la integridad de la intención de voto desde su emisión hasta su registro y contabilización.
- El sistema debe proveer un mecanismo claro de votación, que no genere confusiones al usuario, de manera que pueda prestar su voto de manera asertiva.
- El sistema, así como el proceso de elección, debe ser completamente auditable, antes, durante y posterior a la realización de la sesión electoral.
- Es necesario que solo puedan votar los usuarios autorizados para hacerlo, y que sólo lo puedan realizar una sola vez.
- Permitir que solo los usuarios autorizados puedan participar de la votación en la medida en la que estén autorizados.

Por otra parte, los factores políticos, sociales y económicos también son de gran influencia en la adopción y/o implementación de un cambio. En ese sentido, surgen una serie de condiciones adicionales que debería cumplir un sistema de este estilo:

- Ser de código abierto (open source), lo cual permitirá que el proceso de auditoría, no solo involucre al proceso electoral, sino también al mecanismo que lo sustenta.
- El sistema debe ser de bajo costo, tanto de adquisición (compra), como de implementación, operación y mantenimiento.

Finalmente, el sistema posee una serie de requisitos deseables, cuya implementación le otorgaría mayor flexibilidad y uso:

- Permitir que se puedan llevar a cabo elecciones con sufragio público y elecciones con sufragio secreto.
- Permitir que existan elecciones ponderables.

Teniendo en cuenta las condiciones planteadas a las que debe adaptarse el sistema, ¿por qué se plantea el uso de blockchain?. Para responder esta pregunta, se debe hacer un breve repaso por la definición de blockchain. Blockchain[4], o también llamada "cadena de bloques", es a fines prácticos, una base de datos distribuida entre todos los nodos de una red (todos los nodos tendrán una copia exacta de la misma información) donde los registros se organizan en estructuras llamadas bloques, los cuales se encadenan entre sé mediante un índice hash, es decir, cada bloque tiene el código hash del bloque predecesor en la cadena. Esto permite que, si un bloque es alterado, el código hash de dicho bloque se modifique y en consecuencia la cadena se rompa. Otra consecuencia de esto, es que solo se pueden realizar transacciones de inserción, no de edición ni de eliminación. Esta tecnología digital surge como idea en 1991, con el propósito de firmar documentos digitales con un sello de tiempo para evitar que los mismos fueran manipulados, utilizando criptografía.

En 2004, se formaliza el concepto de "Proof of Work" (PoW)[13], el cual provee un sistema de autenticación alternativo y descentralizado. Por este medio, el cliente debe realizar una serie de ejercicios computacionales que le demandarán un determinado esfuerzo (el cual, a fines prácticos, se reduce en tiempo de computación), para verificarse ante un proveedor. Cabe destacar que para este proveedor, la verificación del PoW realizado por el cliente, es muy baja en cuanto a costo computacional. El mecanismo PoW posibilita en blockchain, la validación de los registros que se agruparán en un bloque y la inserción exitosa del mismo a una cadena.

Sustentado en estos conceptos, surge en 2009 la famosa criptomoneda "Bitcoin", cuya popularidad daría origen a un sistema de economía digital, descentralizada, cuyo valor aumentaría al ritmo de su popularidad.

Posteriormente, en 2015, surge "Ethereum"[14], una plataforma digital que, al igual que Bitcoin, propone una blockchain pero con la diferencia que la misma es programable. Los desarrolladores ahora pueden generar sus propios "contratos

inteligentes" (smart contracts), los cuales consisten en piezas de software capaces de ejecutarse de manera automática ante el cumplimiento de determinadas condiciones, ofreciendo una salida determinada de acuerdo a la entrada recibida. De esta manera, los contratos inteligentes brindan confianza a las partes implicadas en un contrato o acuerdo de partes, el cumplimiento de los términos y condiciones planteadas, o la ejecución de las penalidades en caso de que no. A partir de ahora, existe la posibilidad de desarrollar aplicaciones que garanticen su credibilidad en función del uso de la blockchain, mediante el almacenamiento de sus activos en la misma, de manera distribuida. A estas aplicaciones se las conoce como "DApps" (Descentralized Applications).

2.2. Ventajas y Desventajas de la Blockchain

Ahora bien, puede surgir la pregunta ¿qué tan segura es la blockchain?. Para responderla se debe tener en consideración que la distribución de la información en múltiples nodos de la red proporciona una redundancia de información, donde la veracidad de la misma se verifica de manera democrática en mayoría simple. Esto implica que, si un atacante procura introducir cambios en los registros de un bloque, debe modificar de manera simultánea la mitad de los nodos + 1, de esta forma, su cambio sería validado por la mayoría de los nodos, y en consecuencia, por la red entera. Ahora bien, esto es, a fines prácticos, muy costoso de conseguir. Esta misma redundancia de información, posibilita que el sistema no se caiga por la no disponibilidad de un determinado nodo de la red. Por otra parte, el mecanismo PoW impide que un atacante intente introducir registros adulterados y a su vez, impide los ataques de denegación de servicio.

¿Qué desventaja tiene la blockchain?. La distribución de la información en múltiples nodos implica, para todos esos nodos, un alto costo de almacenamiento. Por otra parte, la resolución de los algoritmos del mecanismo PoW que permite la adición de nuevos bloques a la cadena demanda mucho costo computacional. Existen nodos en la red, que se encargan de realizar estos complejos cálculos, compitiendo entre sí para agregar cada uno de los bloques a la cadena, a cambio de un incentivo económico (en las comunidades formadas en torno al Bitcoin, se conoce como mineros a las personas que disponen de hardware lo suficientemente eficaz, para utilizarlas en servicio del procesamiento de los cálculo, a fin de obtener bitcoins). Comúnmente, este incentivo es premiado en criptomoneda asociada a la blockchain para la cual trabaje, por ejemplo Bitcoin, Ethereum, Dogecoin, entre otras. Sin embargo, esta actividad implica un gasto eléctrico muy importante, lo que a la larga se traduce en un mayor impacto medioambiental. No obstante, existen implementaciones de blockchain que combinan diferentes estrategias para mitigar las distintas desventajas antes mencionadas. Tal es el caso de la Blockchain Federal Argentina.

2.3. Blockchain Federal Argentina

Blockchain Federal Argentina (BFA)[4] es un proyecto originado en 2019, cuya misión es desplegar una red blockchain a nivel nacional y disponibilizar, de manera gratuita, dentro de un espacio colaborativo, todas las bondades que ofrece la blockchain. BFA fue implementada utilizando el framework de Ethereum, sin embargo, a diferencia de los modelos más conocidos de blockchain en el mundo, no se utiliza autenticación de tipo PoW, sino que se utiliza Prueba de Autoridad (PoA), en la cual existe un conjunto confiable de nodos selladores autorizados, eliminando la necesidad de nodos anónimos que compitan para sellar bloques. Estos nodos autorizados, están distribuidos en organismos estatales, académicos, sociales, industriales y comerciales. Esta característica implica la reducción del costo de utilización y sellado a un nivel marginal, lo cual la convierte en una plataforma gratuita de uso. Así mismo, para disminuir el costo de mantenimiento, el modelo de almacenamiento utilizado por BFA es off-chain, esto es, BFA no almacena documentos o archivos, ni ningún tipo de información, sino que guardará los códigos hash de los mismos. De esta forma, la cantidad de espacio requerido por parte de los nodos se reduce enormemente. La responsabilidad de almacenamiento de los documentos será de los clientes de la red. De todas formas, aunque no se almacene el documento completo, el almacenamiento de su código hash resulta suficiente, ya que BFA provee un mecanismo denominado "sello de tiempo" o TSA por sus siglas en inglés, a través del cual un documento se certifica y se asocia a su fecha y hora de certificación. Posteriormente, cuando se quiera corroborar su legitimidad, se puede demostrar o evidenciar que el documento ha permanecido inalterable a partir de la fecha y hora de certificación. Este servicio está disponible a través de una GUI, una API REST y a través de un Smart Contract. Por otra parte, al ser BFA un proyecto nacional, sus referentes y su equipo técnico están disponibles, a su vez que la Universidad Nacional del Comahue, podría dar contribución a la Soberanía Tecnológica.

Todas estas características presentes en BFA la hacen especialmente interesante, adecuada y sinérgica para el proyecto de un sistema de votación universitario del tipo BBB-Voting, y por esta razón es que se la menciona y detalla brevemente sus bondades.

3. Sistemas de Voto Online existentes

Una de las primeras etapas de implementación consiste en la revisión de las ofertas existente sobre sistemas que cumplan con los requerimientos planteados, o en su defecto, con la mayoría. También son considerables aquellos sistemas que, pese a no cumplir con todos los requisitos necesarios, puedan ser factibles de modificar/adaptar. Se realizará una comparación entre ellos y, en caso de no ser factible el utilizar un sistema armado, se planteará la implementación de un nuevo sistema. Para ello, se describirá una meta arquitectura que puede satisfacer los requerimientos propuestos.

[4] https://bfa.ar/

3.1. Open Vote Network (OVN)

Open Vote Network (OVN) [8] es un sistema desarrollado por la Universidad de Newcastle, presentado como la primera aplicación de votación por Internet (e-voting) que permite la máxima privacidad de votante por la utilización de un protocolo descentralizado. El sistema utiliza Smart Contract sobre la Blockchain Ethereum.
En el sistema OVN utiliza el protocolo descripto en [6], que le permite a cada votante tener el control de la privacidad de su voto. La única forma de que pueda ser violado el secreto de los votos es por complicidad total de todos los votantes.

3.2. Platform-Independent Secure Blockchain-Based Voting System (PISBBV)

Los autores del artículo [15] proponen un sistema de votación seguro, verificable e independiente de la plataforma que puede ser desplegada en cualquier blockchain que soporte la ejecución de smart contracts. De esa forma, este sistema sortea el problema de tener que depender de una autoridad central para el conteo y control de los votos, y al no depender de un blockchain determinado, la seguridad puede ser personalizada. En este trabajo los autores emplearon el sistema de Blockchain Hyperldger Fabric[5] donde se implementan además técnicas de cifrado Paillier[6], proof-of-knowledge[5] y linkable ring signature[7] que son utilizadas para dar un marco de seguridad al sistema y privacidad al usuario dentro del nuevo blockchain.
Además, el sistema de voto no depende de una autoridad central para el conteo y la publicación de los votos. Toda la información es calculada automáticamente sin revelar quién es el autor del voto.
Por otro lado, el sistema es escalable ya que con la aplicación de los algoritmos de Linkable Ring Signature se consigue una latencia muy baja. Los autores hicieron un prueba exitosa de rendimiento con un millón de votantes virtuales para demostrar la escalabilidad.

3.3. AppSamblea

AppSamblea [8] [1] es probablemente, una de las aplicaciones de votación online, más completa del mercado. Cuenta con verificación de identidad en distintos niveles de confiabilidad de acuerdo al plan que se contrate. Cuenta con personalización básica y avanzada de los comicios a desarrollar. En la modalidad de pago, cuenta con soporte para votaciones personalizadas. A si mismo, la versión premium cuenta con soporte en blockchain (las versiones básicas no), así

[5] https://www.hyperledger.org/use/fabric
[6] https://www.sciencedirect.com/topics/computer-science/paillier-cryptosystem
[7] https://link.springer.com/chapter/10.1007/11424826$_6$5
[8] https://appsamblea.com/

como formación, consultoría y soporte instantáneo. Al constituir un desarrollo comercial, esta aplicación debe necesariamente ser licenciada, lo cual se traduce en un costo económico de operación y mantenimiento. A su vez, de acuerdo a la licencia contratada, serán las distintas características del sistema desbloqueadas.

3.4. Sistema de votación del Congreso de la Nación Argentina

Unos de los casos de uso planteados por BFA es el sistema desarrollado en el Honorable Congreso de la Nación Argentina, en el cual el sistema permite la realización de las votaciones online, autenticando a los usuarios (diputados y senadores) a través del sistema Autenticar Federal[9]. Luego de que cada usuario emite su voto, los resultados son sellados por la BFA y luego almacenados. Este sistema resulta interesante de mencionar ya que es muy similar al sistema que se plantea desplegar en el entorno académico.

3.5. Comparación

Considerando los sistemas presentados, se elabora la Tabla 1 comparativa entre los mismos para contrastar las principales características deseadas.

	OVN	PISBBV	AppS	Congreso
Integridad de Voto	x	x	En versiones licenciadas	x
Facilidad de Uso	-	-	x	x
Auditable	x	-	-	x
Autenticación de Usuarios	-	-	En versiones licenciadas	x
Open Source	x	-	-	-
Bajo Costo	-	-	-	-
Voto Público y Privado	-	-	En versiones licenciadas	x
Voto Ponderable	-	-	En versiones licenciadas	-

Tabla 1: Comparación de sistemas de votación tipo BBB-voting

Como resultado de la comparación, se puede notar que ninguno de los sistemas planteados resuelve la totalidad de las condiciones mínimas que se requiere para ser desplegado con éxito en un entorno académico. Sin embargo, es posible explorar OVN (dada su característica Open Source) como framework a fin de evolucionarlo hasta conseguir un MVP (por sus siglas en inglés: Minimum Viable Product).

[9] https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/autenticar

Respecto a OVN, la implementación fue realizada dentro de la Blockchain pública de Ethereum donde por limitaciones en el tamaño del código se dividió en 2 Smart Contracts: Un contrato de voto (VoteCon) con la lógica del protocolo y un contrato de criptografía (CryptonCon) que contenía el código para crear y verificar los Zero Knowledge Protocol (ZKP)[5] que tiene el protocolo propuesto. La experimentación consistió en simular la votación con 40 participantes en computadoras MAC arrojando un costo de 32 dolares (sobre plataforma Ethereum).

Los fuentes de Open Vote Network se encuentran disponibles en el repositorio público [10] bajo licencia MIT [11].

Por otra parte este trabajo propone un protocolo descentralizado de dos rondas[6]. En la primera ronda todos los votantes registran su intención de votar y en la segunda los votantes registrados en la primera ronda emiten su voto. El protocolo le permite a cada votante tener el control de la privacidad de su voto, así como también la posibilidad de verificación del mismo. El protocolo tiene la propiedad de auto-conteo, lo que permite que cualquiera, votantes y no votantes, puedan ver y contar todos los votos sin saber quien votó a cada quien, asegurando la integridad y fiscalización del resultado. En el trabajo se propone un sistema para dos opciones de voto, pero se podría extender a más opciones. Un sistema denominado BBB-Voting [12] plantea una evolución de OVN donde permite una elección no binaria.

Un posible riesgo que conlleva el procedimiento propuesto en este trabajo, es que si en la segunda vuelta no votan todas las personas registradas en la primera sería posible invalidar la elección. Otro riesgo es que el último votante podría saber el resultado de la elección, sin haber emitido su voto pudiendo definir la elección a su criterio.

Como se ha mencionado, y para concluir esta sección, OVN es factible de ser utilizado como core del sistema, sin embargo, requeriría muchas modificaciones, entre ellas (y tal vez una de las más importantes) es cambiar el uso de Ethereum por BFA, lo cual permitiría disminuir los costos de uso y mantenimiento.

4. Propuesta

Dado que los sistemas planteados, no terminan de ajustarse al dominio por no cumplir con la totalidad de las características deseadas, se propone invertir esfuerzos en la confección de un nuevo sistema.

4.1. Arquitectura

Para hacer frente al desafío que implica el desarrollo de un sistema que cumpla con los estándares propuestos, se plantea una arquitectura basada en microservicios[2]. Se apuesta fuertemente a la sencillez y a la escalabilidad a largo plazo. Por un lado, los diferentes usuarios podrán interactuar con un frontend

[10] Repositorio git UVN: `https://github.com/stonecoldpat/anonymousvoting`
[11] Licencia MIT: `https://choosealicense.com/licenses/mit/`

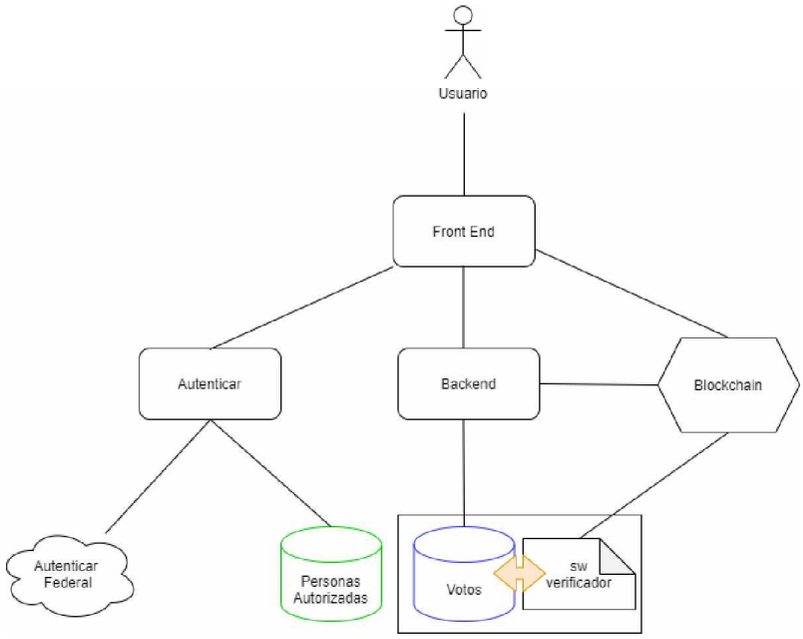

Figura 1: Arquitectura del Sistema Propuesto

en forma de webapp, el cual realizará la autenticación mediante el uso de un servicio que podrá utilizar el sistema de autenticación federal .^Autenticar"[12] para autenticar a los usuarios, y mediante la consulta a una base de datos interna de usuarios, se podrá determinar que el usuario es quien dice ser, y a su vez determinar el rol y los permisos que el mismo posee.

Cabe destacar que el sistema permitirá, no solo tener usuarios habilitados para la votación, sino también para la auditoría de los procesos, sin embargo, se centrará la explicación de la arquitectura en función del caso de uso principal del sistema: emitir un voto.

Por un lado, el usuario previamente designado como elector, interactuando con el frontend podrá seleccionar la sesión de decisión a la cual desea asistir. Expresará su intención de voto. El frontend generará un documento PDF, mostrando el voto expresado por el usuario a fin de obtener validación. Posteriormente, el sistema generará un código hash y solicitará a la blockchain federal la firma del mismo. En este sentido, la blockchain guardará el hash del documento validado por el usuario con su intención de voto. Así mismo, el backend (donde podría residir el core de OVN) recibirá la petición de voto por parte del frontend (PDF), el backend generará el código hash del mismo y consultará a la blockchain la validez de la cadena. Si la validación resultara incorrecta, es porque el

[12] https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/autenticar

documento PDF se encuentra corrupto. Caso contrario, el backend procederá a la computación del voto y persistirá el resultado. Cabe destacar, que el backend tiene la capacidad de, obtenido el resultado final de la elección, generar un archivo PDF, generar un código hash para el mismo, y a su vez firmarlo en la blockchain.

De esta forma, podrá persistir en la base de datos, no solo los votos individuales, sino también el resultado propio de la elección en un documento PDF cuyo código hash estará firmado en la blockchain.

A si mismo, una pequeña pieza de software, de manera autónoma, realizará de manera periódica validaciones sobre los registros de la votaciones. Esto es, tomará los documentos PDF almacenados, generará el hash de cada uno, y verificará con la blockchain que el mismo no esté corrupto. Es importante que esta pieza de software esté ejecutando en el mismo entorno de ejecución que el sistema de bases de datos, de forma que se pueda minimizar el riesgo de que la comunicación entre los mismos pueda ser interceptada.

En la figura 1, se muestra un esquema de la arquitectura propuesta.

4.2. Auditoría

El sistema permitirá que usuarios no electores puedan auditar el proceso de votación, sabiendo en tiempo real el resultado y el proceso. A la vez, puede verificar por si mismo la validez de los votos chequeando contra la blockchain su validez. A si mismo, verificando los resultados generados por el software verificador. Esto permitiría cumplir con la condición número 4 planteada en la sección 2.1, permitiendo que el sistema sea auditable en cualquier etapa.

4.3. Seguridad

La seguridad de la aplicación es abarcada en tres grandes aspectos arquitectónicos. Por un lado, seguridad a nivel usuario, permitiendo identificar que el usuario que se autentica es quien dice ser. Esto cumpliría con la condición de que el sistema debe asegurar la integridad de la intención de voto. Por otra parte, seguridad a nivel aplicación, restringiendo las operaciones habilitadas para cada usuario en función de un rol determinado. Y finalmente seguridad abstracta de la red, al tener un sistema de chequeo de la integridad de los votos en todas las capas de la aplicación.

4.4. Alternativas de implementación

Una de las alternativas de implementación del sistema podría consistir en la utilización de firma electrónica de los votos a través de un token de seguridad. El problema de la autenticidad de los usuarios sería resulta a través de la posesión de un token único que permita al usuario firmar su voto. Luego, el backend validaría la firma generada y computaría el voto. Tras la computación de los votos, el sistema enviaría el resultado de la elección a un usuario que oficie como

autoridad electoral para que los valide y firme utilizando su firma electrónica. De esta forma, es posible evitar el uso de blockchain y obtener autenticación, autenticidad y validación a través de una autoridad certificante.

5. Conclusiones y Trabajos Futuros

Como resultado del proceso de investigación, es posible concluir, que la implementación y despliegue de un sistema de votación online para entornos académicos, corporativos y organizacionales, seguro, con resguardo de la privacidad, auditable y a bajo costo es, no solo factible, sino también necesario. Esto es posible gracias a la utilización de blockchain como sustento principal de los mecanismos de auditabilidad. Cabe destacar que, al tratarse de un sistema tipo Blockchain-Based Boardroom Voting, su alcance y aplicación está limitado a entornos de votación relativamente pequeños, y bajo ninguna circunstancia este documento avala la aplicación de sistemas de voto online en entornos más grandes, tales como procesos electorales políticos llevados a cabo en una ciudad, provincia o a nivel nacional, sin una correspondiente investigación previa que lo avale[3].

Como trabajo futuro, se procederá a instalar una instancia de OVN a fin de verificar sus funcionalidades. Posteriormente se analizará el código de la herramienta a fin de verificar que tan factible es de modificar y evolucionar. Se llevará a cabo el despliegue, en un entorno de pruebas, del resto de los componentes arquitectónicos y el sistema resultante será puesto bajo evaluación en el Consejo Directivo de la Facultad de Informática de la Universidad Nacional del Comahue. Cabe destacar tanto el sistema, así como toda la documentación asociada, será publicada bajo licencia GNU[13].

Referencias

1. R. Bejarano Parrilla. Sistema de voto electrónico mediante autenticación con dnie. B.S. thesis, 2017.
2. D. A. B. Contreras. Arquitectura de microservicios. *Tecnología Investigación Y Academia*, 6(1):36–46, 2018.
3. C. N. de Investigaciones Científicas y Técnicas. Análisis de factibilidad en la implementación de tecnología en diferentes aspectos y etapas del proceso electoral `https://www.conicet.gov.ar/wp-content/uploads/Analisis_factibilidad_implementacion_tecnologia_proceso_electoral.pdf`. Accedido 31-10-2020.
4. M. Di Pierro. What is the blockchain? *Computing in Science & Engineering*, 19(5):92–95, 2017.
5. U. Feige and A. Shamir. Zero knowledge proofs of knowledge in two rounds. In *Conference on the Theory and Application of Cryptology*, pages 526–544. Springer, 1989.
6. F. Hao, P. Y. Ryan, and P. Zieliński. Anonymous voting by two-round public discussion. *IET Information Security*, 4(2):62–67, 2010.

[13] https://www.gnu.org/licenses/licenses.es.html

7. P. Kogan, S. Soto, and C. A. Vaucheret. Aportes al proceso de fiscalización electrónica: experiencia sobre uso de la boleta única electrónica en elecciones 2019, provincia de neuquén. In *XIII Simposio de Informática en el Estado (SIE 2019)-JAIIO 48 (Salta)*, 2019.
8. P. McCorry, S. F. Shahandashti, and F. Hao. A smart contract for boardroom voting with maximum voter privacy. In *International Conference on Financial Cryptography and Data Security*, pages 357–375. Springer, 2017.
9. J. S. Preisegger, R. Muñoz, A. C. Pasini, and P. M. Pesado. Blockchain y gobierno digital. In *XXV Congreso Argentino de Ciencias de la Computación (CACIC)(Universidad Nacional de Río Cuarto, Córdoba, 14 al 18 de octubre de 2019)*, 2019.
10. A. Prince, L. Jolías, and F. Lacabanne. Voto electrónico en argentina. In *VI Simposio de Informática en el Estado (SIE 2012)-JAIIO 41 (CABA, 2012)*, 2012.
11. S. Soto, C. Ramos, P. Kogan, C. A. Vaucheret, and J. Rodríguez. Gukena: escrutinio descentralizado para voto ponderado. In *XII Simposio de Informática en el Estado (SIE 2018)-JAIIO 47 (CABA, 2018)*, 2018.
12. S. Venugopalan, I. Homoliak, Z. Li, and P. Szalachowski. Bbb-voting: 1-out-of-k blockchain-based boardroom voting. *arXiv preprint arXiv:2010.09112*, 2020.
13. I. Villameriel Martínez et al. Blockchain y criptomonedas. 2019.
14. G. Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.
15. B. Yu, J. K. Liu, A. Sakzad, S. Nepal, R. Steinfeld, P. Rimba, and M. H. Au. Platform-independent secure blockchain-based voting system. In *International Conference on Information Security*, pages 369–386. Springer, 2018.