Blockchain en la Lotería de Río Negro

Primera Lotería en el mundo en utilizar esta tecnología

Índice

1. Introducción

La Lotería de la Provincia de Río Negro se encuentra en un proceso de innovación constante, con el objetivo de optimizar sus procesos, elevar sus niveles de transparencia y brindar mejores servicios, todo esto en el marco de la utilización de las tecnologías de la Cuarta Revolución Industrial. Bajo esta premisa, se ha comenzado un proceso de investigación y análisis de la posibilidad de utilización de la tecnología blockchain en diversos procesos de la Lotería, objeto por el cual se desarrolla el presente informe.

El objetivo del documento es analizar las características de esta tecnología, sus aplicaciones en el ámbito del Sector Público, sus posibles impactos en la gestión de la información de la Lotería, así como un análisis de viabilidad de una prueba piloto. La tecnología blockchain surgió en el 2008 y es conocida por ser la tecnología que permite las transacciones del Bitcoin. En resumidas cuentas, blockchain es una tecnología de confianza que, gracias a sus características, permite que dos extraños puedan intercambiar bienes o valor sin la necesidad de contar con un intermediario (en el caso de las criptomonedas, un banco). Una de las funciones sociales de las instituciones es la de brindar confianza sobre transacciones, procesos o intercambios.

Además de instituciones, existen tecnologías de confianza que complementan el trabajo de profesionales u organizaciones. El ejemplo más simple es el del papel carbónico: este papel permite hacer copias de un mismo documento o información al instante, asegurando que, por ejemplo, todos los involucrados tengan la misma copia de un contrato. El papel carbónico ha sido un invento que dio confianza a las partes involucradas, ya que no es lo mismo tener la misma copia al instante, al momento de la redacción, que copiar a mano un mismo documento dos veces. Los involucrados tienen la seguridad que la información contenida en ese registro (ledger) es exactamente la misma, dando integridad a los datos y confianza a las partes. El blockchain es al igual que el papel carbónico, una tecnología de confianza. Básicamente es una base de datos distribuida donde se lleva registro de cada transacción o intercambio que se realice. Lo innovador de blockchain es que el registro se encuentra distribuido en cada uno de los integrantes que forman parte del proceso y al no ser una base centralizada,es imposible su modificación, ya que una vez que un dato ha sido publicado y enlazando a un bloque anterior, el bloque es validado por toda la red en tiempo real, dando confianza y certeza a todos los nodos integrantes de la red (función clave de esta tecnología). Además es gracias a este encadenamiento es que se pueden ordenar los eventos en el tiempo, de modo de brindar trazabilidad y transparencia a cualquier tipo de procesos. Mediante el uso de blockchain, computadoras de entidades autónomas siguen un protocolo criptográfico para validar transacciones realizadas por los integrantes de esa red, las cuales quedan registradas en una base de datos común y distribuida. A su vez, dependiendo de los permisos, las partes pueden modificar o agregar información en el documento, al tiempo que estos cambios son vistos por todos los involucrados. Este proceso de autenticación distribuida significa que la cadena de bloques no sólo es inalterable sino inmutable. Existe en múltiples lugares a la vez, por lo que no es posible que un error o una falsificación se apodere, además de que todos los cambios realizados serán visibles públicamente por todas las partes involucradas.

¿Por qué blockchain puede impactar positivamente en el Estado? Porque éste se sustenta en la burocracia y la burocracia es principalmente un registro (ledger). Un ledger confirma hechos: cuando existen dudas o no existe consenso, vamos al registro.En el Estado uno ve registros por todos lados. ¿Qué certifica mi nacionalidad, la propiedad de mi casa o mi identidad? Una gran base de datos que administra el Estado. Los registros de propiedad asignan quién posee qué y si su tierra está sujeta a determinadas normas o gravámenes. El registro de nacimientos, muertes o matrimonios certifica la existencia de individuos en momentos claves de su vida y utiliza esa información para confirmar identidades cuando esas personas interactúan con otros. La ciudadanía es una gran base de datos que registra quién tiene derechos y está sujeto a las obligaciones derivadas de la nacionalidad. Lo que no existe en un ledger, no existe para el Estado. De allí que pensar en registros o ledgers distribuidos sea una novedad en los ámbitos de gobierno. Blockchain podría hacer más eficiente la forma en la cual se gestionan los registros públicos, además de mejorar la interoperabilidad de la Administración Pública.

Como se mencionó anteriormente, el Blockchain agrega seguridad a la información, ya que al ser una base de datos distribuida es casi imposible alterar o hackear la información contenida en la cadena. En segundo lugar cabe destacar la integridad, ya que garantiza que los datos no han sido modificados desde su creación sin el consentimiento de los que participan del proceso. Asimismo, y a diferencia de la firma digital, el blockchain permite además certificar la existencia de un documento o archivo. Los datos contenidos en la cadena de bloques vienen con su propia historia y la historia es una parte fundamental para probar su integridad; esta es una cualidad muy poderosa. La procedencia digital, es decir, la prueba de que se produjo un evento digital, es el aporte más valioso de esta tecnología. Otra de las fortalezas es que permite simplificar la trazabilidad de un proceso, pudiendo auditarse de manera más simple, lo que a su vez otorga transparencia, de modo que terceras partes pueden auditar y controlar el accionar del Estado gracias a la información distribuida del blockchain.

Teniendo en cuenta la potencialidad de esta tecnología, la Lotería de la Provincia de Río Negro elabora el presente informe con la finalidad de dar a conocer su experiencia en la utilización de blockchain, así como allanar el camino para que otras Loterías puedan realizar sus propias experiencias.

2. Qué es blockchain?

La tecnología blockchain surgió en el 2008 y es conocida por ser la tecnología que permite las transacciones del Bitcoin. En resumidas cuentas, blockchain es una tecnología de confianza que, gracias a sus características, permite que dos extraños puedan intercambiar bienes o valor sin la necesidad de contar con un intermediario (en el caso de las criptomonedas, un banco). Una de las funciones sociales de las instituciones es la de brindar confianza sobre transacciones, procesos o intercambios. Por ejemplo, si yo acepto subirme a un avión piloteado por un completo extraño, es porque confío en que distintas instituciones

(empresa, regulador, Estado, etc.) han evaluado y certificado las condiciones técnicas y psíquicas de ese piloto. Las instituciones me dan confianza que esa persona está capacitada para pilotear el avión, por lo que personalmente confío en el sistema y acepto subirme a ese avión.

Además de instituciones, existen tecnologías de confianza que complementan el trabajo de profesionales u organizaciones. El ejemplo más simple es el del papel carbónico: este papel permite hacer copias de un mismo documento o información al instante, asegurando que, por ejemplo, todos los involucrados tengan la misma copia de un contrato. El papel carbónico ha sido un invento que dio confianza a las partes involucradas, ya que no es lo mismo tener la misma copia al instante, al momento de la redacción, que copiar a mano un mismo documento dos veces. Los involucrados tienen la seguridad que la información contenida en ese registro (*ledger*) es exactamente la misma, dando integridad a los datos y confianza a las partes. El blockchain es al igual que el papel carbónico, una tecnología de confianza. Básicamente es una base de datos distribuida donde se lleva registro de cada transacción o intercambio que se realice. Lo innovador de blockchain es que el registro se encuentra distribuido en cada uno de los integrantes que forman parte del proceso y al no ser una base centralizada, es imposible su modificación, ya que una vez que un dato ha sido publicado y enlazando a un bloque anterior, el bloque es validado por toda la red en tiempo real, dando confianza y certeza a todos los nodos integrantes de la red (función clave de esta tecnología). Además es gracias a este encadenamiento es que se pueden ordenar los eventos en el tiempo, de modo de brindar trazabilidad y transparencia a cualquier tipo de procesos. Mediante el uso de blockchain, computadoras de entidades autónomas siguen un protocolo criptográfico para validar transacciones realizadas por los integrantes de esa red, las cuales quedan registradas en una base de datos común y distribuida. Podríamos hacer una analogía con un google doc o sheet: un google doc nos permite que distintas personas accedan en tiempo real al mismo archivo, de manera que todos tienen la misma información. A su vez, dependiendo de los permisos, las partes pueden modificar o agregar información en el documento, al tiempo que estos cambios son vistos por todos los involucrados. Este proceso de autenticación distribuida significa que la cadena de bloques no sólo es inalterable sino inmutable. Existe en múltiples lugares a la vez, por lo que no es posible que un error o una falsificación se apodere, además de que todos los cambios realizados serán visibles públicamente por todas las partes involucradas.

Cuando hablamos de blockchain estamos hablando de registros digitales distribuidos o DLT (por sus siglas en inglés: Distributed Ledger Technology).[1] Estos blockchain o DLT pueden ser públicos o privados. Los públicos son aquellos que tienen más años de experimentación y se utilizan en gran medida para las criptomonedas. Entre los blockchain públicos más conocidos se encuentran el de Bitcoin y el de Ethereum. Que sean públicos quiere decir que cualquiera puede ser parte de esa blockchain, no se necesitan permisos para participar y son anónimas, por lo que no requieren la identidad de sus usuarios. Una de las características más llamativas de estas blockchain es su mecanismo para generar acuerdos o consensos acerca de una nueva información o "bloque" incorporado a la cadena (cómo se validan las

[1] El término genérico de esta tecnologías es DLT (Distributed Ledger Technology), término que en nuestra opinión es mejor utilizar, ya que blockchain está muy emparentado con las redes públicas (bitcoin o ethereum) y las criptomonedas.

transacciones). No es la finalidad de este paper describir en detalle los aspectos técnicos de la validación, pero a grandes rasgos, se trata de un proceso matemático que es siempre igual en su lógica pero las variables son diferentes y solo puede resolverse probando números al azar hasta dar con el resultado que se busca en ese momento (mecanismo aleatorio). Los que realizan este proceso son llamados "mineros", los cuales compiten entre sí y aportan una gran capacidad de procesamiento al sistema que permite validar las transacciones. Por cada "solución" o validación, los mineros reciben un pago por sus servicios. Básicamente los mineros se encargan de validar las transacciones y reciben una ganancia por ello. Asimismo, cada bloque de información contiene un encabezado que posee, como mínimo, tres conjuntos de datos: a) la información estructurada sobre las transacciones, b) los datos y el *timestamp* en el algoritmo de "prueba de trabajo", c) la referencia al bloque anterior por medio de un hash, lo que permite "encadenar" la información.

Cuadro 1. Diferencias y similitudes entre blockchains públicas y privadas

Diferencias	Similitudes
Modelo de permisos	Arquitectura p2p
Transacciones administradas	Tolerancia al "problema bizantino"[2]
Criptomonedas	Claves criptográficas
Minería	Transacciones limitadas
Anonimato	Lenguajes
Prueba de trabajo	Cadena de bloques de consenso

Fuente: elaboración propia

Los registros privados están menos explorados y son utilizados principalmente en procesos de empresas privadas. Su arquitectura *peer to peer* es similar a las redes públicas, al igual que el lenguaje de programación. La principal diferencia se encuentra en que al ser privados cuentan con sistemas de permisos (solo aquellos "invitados" pueden participar), son identitarias y no necesariamente necesitan de un mecanismo de minería para validar transacciones como sucede con las blockchains públicas. En este caso la validación puede ser por sistemas de votación, u otra forma de validar transacciones acordada por los participantes (firma digital por ejemplo). Al no contar con un sistema de minería, no es necesario tener una criptomoneda que permita recompensar a los mineros que certifican las transacciones, ni tampoco es necesaria la capacidad de cómputo de las redes públicas. Asimismo, la velocidad de las transacciones es mucho mayor, ya que el ecosistema es más pequeño y la cantidad de transferencias mucho menor. Una de las principales debilidades de estas DLT es su capacidad de construir confianza entre sus integrantes. En el caso de las blockchain públicas (Bitcoin y Ethereum por lo menos), su fortaleza está en la gran cantidad

[2] El problema de "los generales bizantinos" es un experimento mental creado para mostrar el dilema de lograr un consenso entre un conjunto de entidades con un objetivo común cuando entre ellas pueden existir traidores, es decir, entidades con objetivos opuestos que intentan obstaculizar el proceso. Uno de los grandes logros que supone Bitcoin es el hecho de ofrecer la primera solución práctica al problema de los generales bizantinos.

de nodos que participan y el anonimato de los mismos. Contar con pocos nodos o nodos que tengan relación entre sí, puede ser una debilidad de las blockchains privadas.

3. Experiencia en la Lotería de Río Negro

Teniendo en cuenta el Referencial IRAM Nro 19, y su punto nro 8 Procesos Operativos, se propone aplicar la tecnología blockchain a los procesos que se detallan a continuación.

Sorteos

Según la norma IRAM mencionada anteriormente, la Lotería debe establecer, implementar, mantener y documentar un proceso de sorteo para sus juegos que:

A. verifique la integridad del archivo de captura de apuestas;
B. se realice bajo condiciones controladas en cada uno de sus pasos, garantizando la transparencia del acto;
C. tenga siempre como objetivo principal obtener el resultado del sorteo;
D. contemple todas las contingencias posibles que resulten de un análisis cuya información documentada debe ser guardada y mantenida;
E. promocione la participación del público y la comunicación a través de más de un soporte de comunicación masiva.

Al aplicar blockchain en los sorteos que realiza la Lotería, será posible asegurar la integridad del archivo de captura de apuestas (punto A), además de promocionar la participación del público ya que cualquier ciudadano puede volverse un "auditor" de los números ganadores. Esta tecnología permitirá verificar la integridad del archivo de captura de apuestas y garantizar la transparencia del acto, entre otros beneficios. Blockchain puede tener un importante aporte para elevar la confianza y la seguridad en los sorteos, dejando de lado toda sospecha y dando la seguridad en que el sorteo es transparente.

Liquidación y pagos de premios

Además, se propone aplicar esta tecnología en la liquidación y pagos de premios, con el fin de asegurar la confidencialidad de los datos del ganador o generar comprobantes de pago de premios mayores a 100 mil pesos, entre otros. Las características de esta tecnología permite digitalizar diferentes procesos que hoy suceden en papel, y dar la seguridad en todo el proceso de pago de premios.

Según el referencial IRAM mencionado, la Lotería debe establecer, implementar, mantener y documentar un proceso de liquidación y pago de premios para sus juegos que:

A. permita la realización de los pagos de premios a los clientes / participantes en función del tipo de juego y cantidad, así como los controles establecidos;
B. asegure la confidencialidad de los datos del ganador según la normativa que aplique.

En definitiva, se considera que estos dos procesos son ideales para la realización de una prueba piloto con la tecnología blockchain, ya que además de elevar los niveles de confianza

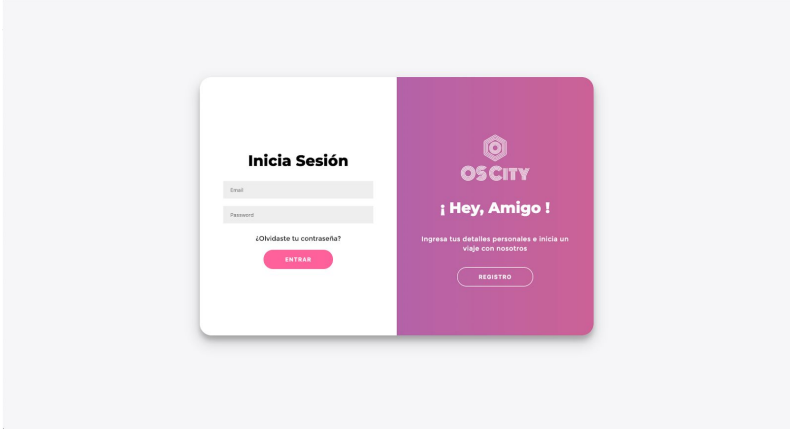
y transparencia de los sorteos, se cumplirán de una manera innovadora las recomendaciones de los protocolos de calidad establecidos por las normas IRAM.

4. Características de la prueba piloto

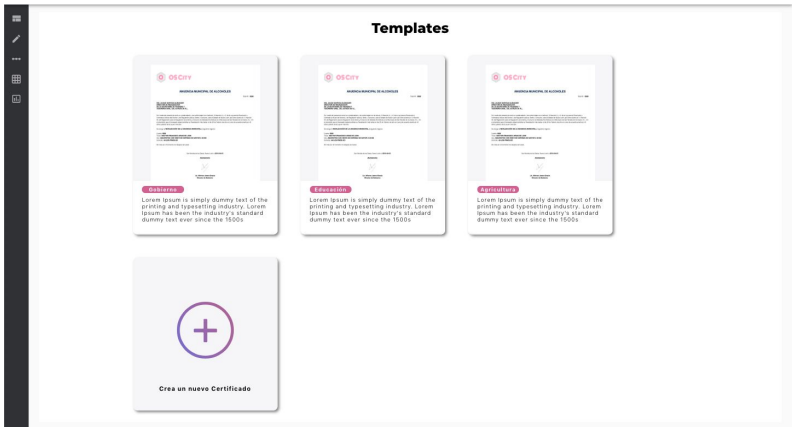
La propuesta tiene como objetivo el desarrollo e implementación de una plataforma que permita registrar los resultados de los sorteos de la quiniela de la Lotería de Río Negro bajo la tecnología blockchain, así como el certificado que emite la institución para aquellos premios mayores a 100.000 pesos.

Para el primer punto, se desarrollará una plataforma que permita al personal de la Lotería registrar el extracto de los sorteos en blockchain, dando como resultado un certificado diario en donde queden registrados todos los números ganadores y se de certeza de su inmutabilidad.

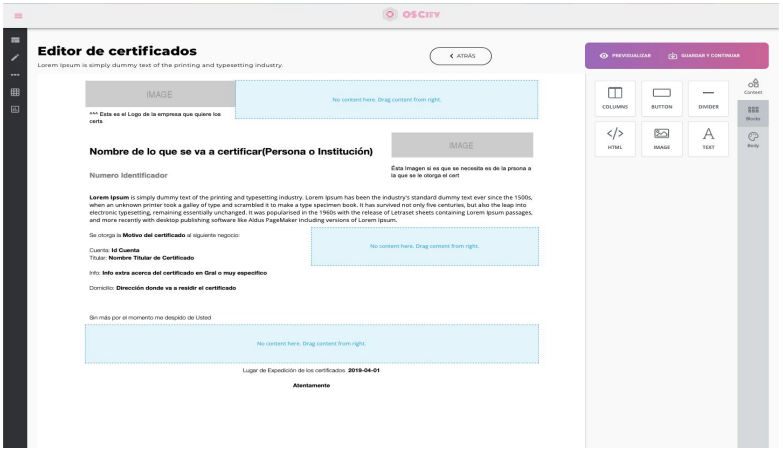
Como se puede observar en las imágenes a continuación, el personal de la Lotería podrá de una manera simple y amigable, certificar los extractos diarios de la Quiniela y emitir sus propios certificados en blockchain. A continuación se muestra el proceso mediante el cual se captura la información y se emiten los certificados en blockchain.



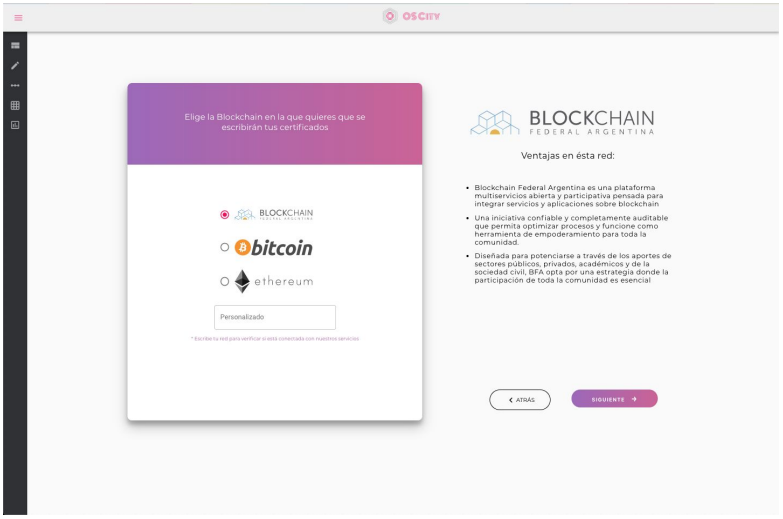
Los usuarios de la Lotería podrán crear sus cuentas y tener acceso a la plataforma.



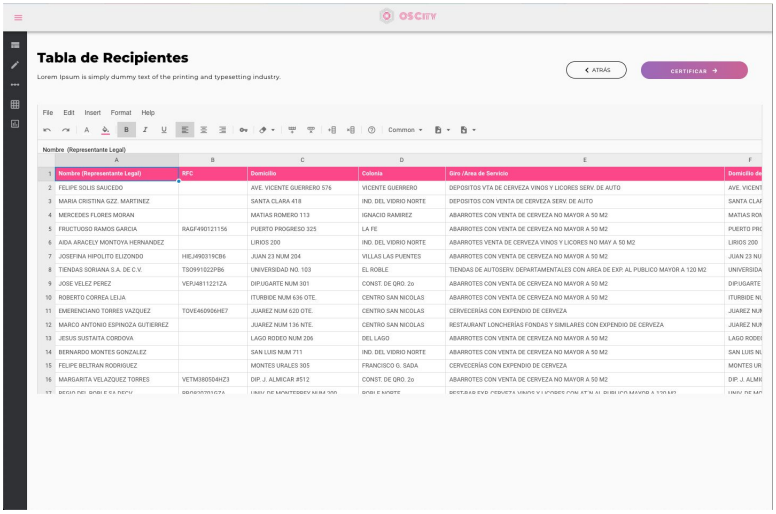
Esta es la primera página que los usuarios verán después de iniciar sesión, aquí eligen una plantilla para sus certificados, los usuarios pueden elegir entre crear una nueva plantilla desde cero o una plantilla existente como guía.



Después de que el usuario seleccione qué plantilla va a usar, podría editar cada parte de esa plantilla y tener todo el control de cómo se verían los certificados, y también podría previsualizarla.



El usuario podrá que elegir qué cadena de bloques desea certificar los certificados. Tiene dos opciones predeterminadas y un campo personalizado. En el backend comparamos la opción seleccionada con nuestros registros y validamos si es posible escribir en la cadena de bloques seleccionada.



Aquí es donde se cargarán los datos, el usuario podría crear una tabla de datos desde cero o cargar un archivo (txt, csv, xls entre otros) y luego modificarlo si lo desea.

Después de que el usuario agrega todos los datos que necesita el certificado y se completa todo el proceso, verá la página de análisis con información sobre la cantidad de certificados y la cantidad de personas que intentaron validar estos certificados.

A su vez, el usuario final podrá acceder a cada uno de esos certificados mediante una interfaz web donde se muestran todos los certificados emitidos con la información de cada extracto. La imagen a continuación muestra el landing inicial, el cual podrá ser alojado en quiniela.loteriaderionegro.gob.ar, en donde el usuario podrá acceder a la información general de la experiencia y un "preguntas frecuentes" en donde se pueda leer la información básica sobre el proyecto, qué es blockchain, sus beneficios y alcances.

En ese mismo landing, el usuario o ciudadano podrá acceder mediante un buscador a todos los certificados emitidos diariamente, desplegando la barra del buscador y eligiendo según la fecha del sorteo.

Una vez seleccionado el certificado, el ciudadano tendrá acceso al certificado en blockchain con el extracto de los 3 sorteos del día de la fecha. En ese mismo certificado, y mediante un solo paso, el usuario podrá verificar que la información del mismo es válida y no ha sido alterada, que el certificado fue emitido por la Lotería y que el mismo no ha sido manipulado. Asimismo, este certificado podrá ser compartido por cualquier medio digital o redes sociales, y cualquier tercero podrá verificar los resultados de la quiniela con la seguridad de que nadie ha manipulado la información.

Esta prueba piloto permitirá mejorar los niveles de eficiencia y transparencia de este proceso, así como dar la certeza de que la información provista por la Lotería no ha sido manipulada ni alterada. Esto sin dudas significa una transformación en los servicios que brinda la Lotería, pero es sólo el comienzo. La tecnología blockchain a resuelto el problema del "doble gasto" en el mundo de las criptomonedas, por lo que también podría ser utilizada para juegos de azar on-line, y para migrar juegos del mundo físico (como la Quiniela) al mundo digital. Esta prueba piloto busca conocer las características prácticas de blockchain y sus implicancias, con la finalidad de poder escalar y ampliar sus aplicaciones.

En resumen, la plataforma permite:

- Generar certificados en blockchain con la información de los extractos diarios de la Lotería.
- Buscar certificados por fecha.
- Realizar analítica sobre los certificados emitidos y sus validaciones.
- Emitir los comprobantes o certificados para aquellos ganadores de más de 100.000 pesos.

Gracias a la solución propuesta, tanto ciudadanos, usuarios de la lotería como auditores del Estado, podrán tener la certeza que la información sobre sorteos y ganadores de la Quiniela no ha sido alterada ni manipulada por nadie. Esto significa un salto tanto en la calidad de la información que gestiona la Lotería como en sus procesos de innovación.

5. Conclusiones

Consideramos que actualmente se está en una etapa primitiva de la utilización de blockchain, y que con el correr del tiempo y las experiencias, podremos avanzar hacia proyectos de mayor impacto en el Estado. Simplificando, uno podría ordenar las etapas de desarrollo del *blockchain* de la siguiente manera: (1) Utilización de *blockchain* públicas como certificadoras o notariado de información o documentos; (2) el desarrollo de apps que permitan el registro e intercambio de certificados o títulos; (3) la generación de *smart contracts* entre el Estado y sus proveedores, (4) la vinculación de *Smart contracts* con bases de datos externas; y (5) la creación de redes privadas entre el Estado, sociedad civil y organismos de control (información pública distribuida). A pesar de la muchas veces exagerada expectativa que existe sobre esta tecnología, no debemos descartar su potencialidad como herramienta de eficiencia y transparencia para gobiernos, en especial para aquellos que necesitan generar mecanismos de confianza entre la administración y sus ciudadanos, o bien agilizar procesos de contralor entre agencias especializadas. De allí que el objetivo de esta consultoría haya sido analizar la viabilidad de aplicación, de manera de poder conocer dónde agrega valor blockchain en la gestión de la Lotería de Río Negro.

Consideramos que un proyecto de aplicación de blockchain en la Lotería de Río Negro, debe reunir las siguientes 5 características:

- Ser un proceso de impacto en la labor de la Lotería y en la transparencia de sus procesos.
- El proceso debe ser lo suficientemente simple como para poder realizar una prueba piloto en un tiempo prudencial.
- Debe poder ampliarse o escalar hacia un proceso completo o hacia otros procesos (salir de la prueba piloto).
- El proceso debe depender exclusivamente de la Lotería, ya que involucrar a otros organismos puede significar mayores obstáculos para la realización de la prueba piloto.
- Debe significar una mejora al usuario final, principalmente a los usuarios de la Lotería y la ciudadanía en general.

Finalmente, el proceso antes descrito podría ser el primer componente para seguir explorando una tecnología de confianza que permita mejorar los servicios que brinda la Lotería, pudiendo escalar a otros procesos y sin grandes complejidades de implementación.