BLOCKCHAIN EN LA ADMINISTRACIÓN PÚBLICA

¿Mucho ruido y pocos bloques?

Florencia Serale · Christoph Redl · Arturo Muente-Kunigami

BID

Banco Interamericano de Desarrollo
1300 New York Avenue, N.W.
Washington, D.C. 20577
www.iadb.org

El Sector de Instituciones para el Desarrollo fue responsable de la producción de la publicación.

Colaboradores externos:
Coordinación de la producción editorial: Sarah Schineller (A&S Information Specialists, LLC)
Revisión editorial: Clara Sarcone
Diagramación: Gastón Cleiman

Parte 1

Implementación de *blockchain* en el sector público

Parte 2

Usos potenciales de *blockchain*

Parte 3

¿Qué es *blockchain*?

Siguientes pasos: menos ruido y más bloques

PRESENTACIÓN

Cada vez más gobiernos de América Latina y el Caribe se enfrentan a un reto similar: necesitan entregar servicios públicos, en cantidad y calidad, de manera eficiente y transparente, y a menudo con menos recursos disponibles. La ciudadanía compara los servicios del gobierno con los que recibe del sector privado, y exige más. Por otro lado, la región sigue mostrando altos índices de desigualdad en términos de distribución de ingreso, se ha convertido en los últimos años en una de las más violentas del mundo y tiene altos índices de corrupción.

Ante esta coyuntura, es fácil pensar que la solución puede provenir de la aplicación de nuevas tecnologías. Después de todo, el gobierno es muchas veces uno de los últimos refugios del trámite basado en papel, los procesos manuales y los sellos. Si bien es cierto que el uso de nuevas tecnologías puede hacer a los gobiernos más eficientes y efectivos, estas no dejan de ser herramientas que deben usarse conociendo muy bien sus potencialidades y limitaciones, y cuya aplicación debe darse siempre acompañada y supeditada a programas de reforma integral.

La aparición de la tecnología de cadena de bloques (*blockchain*) no es la excepción. Su despliegue a nivel mundial como plataforma para el funcionamiento de varias criptomonedas ha creado mucha expectativa respecto del rol que podría desempeñar en otros sectores. De hecho, se ha publicado mucho sobre el potencial que la tecnología podría tener en el sector público, aunque pocas publicaciones ofrecen algún tipo de guía para su implementación. En la práctica, a nivel mundial, son pocos los gobiernos que han implementado algún programa piloto utilizando *blockchain*, y menos aún aquellos que brindan servicios públicos utilizando esta tecnología.

El objetivo principal de esta publicación es ayudar a las administraciones públicas a entender mejor la tecnología, identificar casos concretos en los que su uso podría efectivamente mejorar la prestación de servicios públicos y destacar los principales retos para su implementación. Es importante mencionar que este documento se concentra en el impacto que la tecnología puede tener en el sector público ya que el impacto de *blockchain* –y las criptomonedas en general– sobre los mercados financieros viene siendo evaluada ya por gobiernos y bancos centrales a nivel mundial.

Esperamos que esta publicación sea una contribución valiosa en el proceso de análisis de la tecnología *blockchain* en la administración pública.

Lea Giménez
Jefa de División
Innovación para Servir al Ciudadano
Banco Interamericano de Desarrollo

AGRADECIMIENTOS

Esta publicación incluye los hallazgos y discusiones del seminario *Blockchain Blossom*, realizado en mayo de 2018 como parte de la agenda de conocimiento de la División de Innovación para Servir al Ciudadano (ICS, por sus siglas en inglés) con el apoyo del programa Cutting Edge del sector de Conocimiento, Innovación y Comunicaciones (KIC, por sus siglas en inglés).

Agradecemos a Anna Dusenkova, Ida Uusikyla, Claudia Scuriatti y Jacqueline Bernstein del London School of Economics, quienes proporcionaron insumos para las discusiones de caso de la Parte II

El documento fue revisado por Marcos Allende, del Departamento de Tecnologías de la Información del Banco Interamericano de Desarrollo (BID); Gabriela Andrade, Especialista Líder Mercados Financieros del BID; Lucas Jolías, Director de Prince Consulting; Erika Molina, Especialista del Laboratorio de Innovación del Banco Interamericano de Desarrollo (BID Lab); Alejandro Pareja, Especialista Senior en Modernización del Estado del BID y Fabrizio Scrollini, Director de la Iniciativa Latinoamericana de Datos Abiertos (ILDA). Agradecemos sus comentarios y sugerencias, los cuales hemos tratado de incluir a lo largo de la publicación.

INTRODUCCIÓN

La falta de confianza para hacer transacciones (económicas, jurídicas, burocráticas) ha sido por siglos un problema colectivo que la humanidad ha intentado resolver a través de actores en los que las diferentes partes confían. En muchos casos estos actores se han convertido en instituciones tanto públicas como privadas. Por ejemplo, cuando dos personas que no se conocen desean realizar una transacción de pago electrónico, deben contar con la participación de una tercera parte (como un banco o el emisor de una tarjeta de crédito) para que la transacción se lleve a cabo. De hecho, el gobierno muchas veces tiene que convertirse en un intermediario para validar jurídicamente documentos, probar la identidad de las personas o certificar la elegibilidad para acceder a programas sociales, entre otros.

Recientemente ha surgido una tecnología con el potencial de reemplazar la necesidad de confianza con una prueba criptográfica (Satoshi Nakamoto, 2008). Aplicada en un inicio a transacciones financieras a través de la criptomoneda Bitcoin, la tecnología de cadena de bloques (*blockchain*) puede introducir una lógica distribuida y descentralizada (y bastante costosa) para realizar transacciones de manera segura y confiable sin la necesidad de un tercero que tenga la confianza de los participantes. La adición de los llamados contratos inteligentes (*smart contracts*) facilita la automatización de procesos a través del establecimiento de reglas que se ejecutarán sin la necesidad de intermediarios si se cumplen ciertos requisitos preestablecidos, lo cual, sumado a la confianza que la tecnología promete, plantea en principio desafíos importantes al sector público, cuyas instituciones están acostumbradas a operar en las antítesis de esta lógica. En la actualidad muchos gobiernos están comenzando a explorar la tecnología *blockchain* para proveer mejores servicios. Tal como se menciona a lo largo de esta publicación, pareciera que la situación actual de implementación de soluciones basadas en *blockchain* está generando más ruido que bloques; esto es: si bien son muchos los conceptos y pilotos que se están realizando son pocos los que pasan a una etapa de despliegue a escala. Es muy probable que este bajo nivel de adopción obedezca al estado naciente de la tecnología y a una falta de condiciones habilitantes que permitan escalarla.

Por un lado, es posible que debido al bajo nivel de madurez de la tecnología la mayoría de los proyectos revisados se hayan planteado la pregunta: ¿se puede realizar *esto* con *blockchain*? Este interrogante es adecuado cuando se está aprendiendo sobre una tecnología y por lo tanto es la apropiada en un contexto de experimentación y aprendizaje. Sin embargo, la pregunta que debe hacerse cuando se está pensando en una implementación diseñada para escalar es: ¿cuál es la mejor tecnología que me puede ayudar a solucionar *este problema*? Por otro lado, existen condiciones de tipo legal, regulatorio, tecnológico y de procesos que pueden limitar el despliegue de soluciones basadas en esta tecnología. A medida que la tecnología y su entendimiento por parte de los gobiernos aumenten, seguramente se verán más instancias de aplicación que estén diseñadas para escalar, y se espera que esta publicación ayude en ese proceso.

En general, esta publicación tiene el objetivo de revisar algunas experiencias incipientes, identificar algunos usos potenciales de la tecnología e invitar a reflexionar sobre su potencial para el sector público. La primera parte plantea algunas consideraciones a tomar en cuenta para la implementación de la tecnología *blockchain* en el sector público. La segunda parte propone un marco de análisis para usos potenciales de la tecnología y muestra algunos casos específicos. Finalmente, en la tercera parte se ofrece una explicación muy breve de cómo funciona la tecnología *blockchain*. Si el lector tiene noción sobre los conceptos básicos de la tecnología, se recomienda leer la publicación en el orden que se presenta. En caso de conocer poco sobre la tecnología, se sugiere comenzar por la tercera parte y avanzar la lectura de atrás hacia adelante.

Implementación de *blockchain* en el sector público

1.1. Test

¿Es recomendable utilizar *blockchain* para resolver el problema que tengo?

Esta es de una prueba dirigida a funcionarios públicos que quieran saber si *blockchain* les puede ser útil. Antes de comenzar, se les pide que dejen de lado por un momento la discusión tecnológica y se **concentren en el problema que quieren resolver**. Las preguntas fueron desarrolladas para ayudarlos a entender si *blockchain* puede contribuir o no a solucionar el problema en cuestión.

1. ¿Necesitas que todos los involucrados guarden algún tipo de registro de información?

- ☐ **A /** Sí, todos los usuarios de las entidades involucradas van a generar información que necesita ser registrada.
- ☐ **B /** Sí, pero solo algunos usuarios de algunas entidades van a generar información que necesita ser registrada.
- ☐ **C /** No, solamente un grupo pequeño de una sola entidad generará información que necesita ser registrada.

---

2. ¿Necesitas que todos los involucrados accedan a este registro?

- ☐ **A /** Sí, todos los usuarios de muchas entidades van a acceder al registro.
- ☐ **B /** Sí, pero solo algunos usuarios de varias entidades van a acceder al registro.
- ☐ **C /** No, solamente un grupo pequeño de una sola entidad necesita acceder al registro.

---

3. ¿Alguno de los involucrados tiene incentivos para intentar falsificar la información del registro para sus propios intereses?

- ☐ **A /** Sí.
- ☐ **B /** No.

---

4. ¿Necesitas validar el registro de nueva información en tiempo real o casi real?

- ☐ **A /** No, puedo esperar más de 15 minutos para validar un registro.
- ☐ **B /** No, pero solo puedo esperar hasta 15 minutos para validar un registro.
- ☐ **C /** Sí, necesito que la validación sea inmediata.

---

5. ¿Qué piensas de la existencia de una entidad central que valide/verifique toda la información para confirmar que es legítima y confiable?

- ☐ **A /** No la quiero.
- ☐ **B /** Idealmente no la quiero, pero no me molesta tenerla.
- ☐ **C /** Necesito y quiero una entidad así.

---

6. ¿Necesitas contar con registro histórico confiable de la información para auditarla o rastrearla?

- ☐ **A /** Sí.
- ☐ **B /** No.

---

7. ¿Necesitas que para acceder a la información registrada se siga algún proceso de validación o se consiga algún permiso?

- ☐ **A /** No.
- ☐ **B /** Sí.

---

*Si respondiste **(a)** en todas las preguntas, una solución sobre un* blockchain *público no permisionado puede ayudarte. Si tus respuestas están entre **(a)** y **(b)**, entonces otro tipo de* blockchain *podría ser apropiado. Si respondiste **(c)** en alguna pregunta, es probable que* blockchain *no te sea de mucha utilidad en comparación a otras opciones. Independientemente de este ejercicio, recomendamos explorar otras tecnologías y comparar sus beneficios con los de* blockchain.

1.2.
Consideraciones para su puesta en funcionamiento

Introducir nuevas tecnologías en el sector público puede ser una tarea compleja, que requiere generar capacidades al interior de la administración y reglas de juego claras para su adecuada implementación y, sobre todo, sentar las bases –regulatorias, presupuestarias, políticas– para su sostenibilidad. En la actualidad varias experiencias que utilizan la tecnología *blockchain* consisten en pilotos implementados de forma aislada, con poca relación con otras instituciones públicas y en muchos casos desplegados en paralelo al proceso de diseño de políticas públicas (Zambrano, 2018) y al marco legal y regulatorio vigente. En parte esto puede deberse a la falta de madurez de la tecnología, que impide utilizar todos sus atributos a gran escala por cuestiones como la velocidad de las transacciones, el consumo de energía y el tamaño de los bloques (McKinsey, 2018). Sin embargo, tal como se describe en la segunda parte, varios de estos pilotos han generado incentivos positivos para fomentar la innovación pública, la eficiencia en la prestación de servicios y la digitalización de los sistemas.

Diversos estudios que analizan el uso de la tecnología *blockchain* se han centrado en evaluar la viabilidad de su implementación (WEF, 2018; Berryhill, Bourgery y Hanson, 2018; Yaga et al., 2018; AGESIC, 2018; Wust y Gervais, 2017) y los aspectos de diseño a considerar (Verhulst, 2018; ACT-IAC, 2018; Berryhill, Bourgery y Hanson, 2018; UE, 2018a; Hileman y Rauchs, 2017). Esta primera parte de la publicación se dedica a estudiar los desafíos de implementación para el sector público y analiza los retos de adopción, las condiciones sobre las cuales la tecnología agrega valor público y las precondiciones para una implementación sostenible.

1.2.1. ¿Cuáles son los retos a los que la tecnología se enfrenta para su adopción en el sector público?

Tal como se puede leer en el resto de esta publicación, bajo ciertas condiciones la tecnología *blockchain* puede agregar valor para resolver problemas públicos. *Blockchain* puede convertirse en una solución disruptiva para los gobiernos, dado que habilita el diseño de una lógica distribuida y descentralizada en la provisión de servicios públicos (Zambrano, 2018). En definitiva, algunas funciones de los gobiernos pueden llegar a desaparecer gracias a *blockchain*, tales como registrar eventos (el cambio de propiedad de un vehículo o un inmueble), verificar hechos (por ejemplo, comprobar el pago de impuestos u otorgar credenciales de educación) y constatar el cumplimiento de normas (certificados de sanidad para restaurantes, entre otros) (Torregrossa, 2018). Sin embargo, la implementación de una solución exitosa –y sobre todo sostenible– utilizando tecnología *blockchain* presenta algunos retos: (i) organizacionales y de gobernanza, (ii) tecnológicos, (iii) regulatorios, (iv) de recursos, y (v) de uso y generación del ecosistema.

Retos organizacionales y de gobernanza

Para eliminar la necesidad de intermediaros, la tecnología *blockchain* introduce una gobernanza basada en reglas determinadas en código en forma de un protocolo –esto es, con un mecanismo de consenso, con reglas de validación específicas, y con roles y responsabilidades dependiendo del tipo de actor (si la *blockchain* es privada)–.[1] En la actualidad se dificulta cambiar la gobernanza de manera sistemática (por ejemplo, pasar de una solución basada en Bitcoin a una en Ethereum), porque significa cambiar el código y las reglas de juego establecidas, para lo cual se necesita un consenso de todos los participantes. Para mejorar la flexibilidad de estos cambios y democratizar su uso, actualmente parte de la literatura se centra en analizar cómo diseñar la gobernanza de una solución basada en *blockchain* (Bosankic, 2018; Ehrsam, 2017) que permita una mayor flexibilidad ante cambios en la tecnología. Para el sector público, significa que no solo hay que pensar en qué casos tiene sentido usar la tecnología *blockchain*, sino también planear cómo diseñar la gobernanza de los procesos y de la solución de manera que se garantice el objetivo inicial.

Los retos organizacionales se refieren al establecimiento de una gobernanza adecuada a la solución tecnológica; por lo tanto, para su definición se deben tener en cuenta los arreglos institucionales tanto dentro como fuera de la cadena. Además de decidir sobre el tipo de *blockchain* a utilizar (pública o privada, permisionada o no), se requiere

[1] La tercera parte de esta publicación explica en detalle cómo funcionan las *blockchain* públicas y las diferencias que existen con las privadas.

analizar los flujos de trabajo, protocolos de validación y responsabilidades de la información ingresada, tipos de participantes y sus respectivos permisos, mecanismos de consenso, y reglas de entrada, salida y verificación inherentes a la solución.

La implementación de una solución basada en la tecnología *blockchain* implica que la red de participantes acuerde una gobernanza que aproveche las potencialidades de la tecnología (consistencia, generación de confianza) y determine las reglas de juego en cuanto a permisos, requisitos de entrada y mecanismos de consenso. Adicionalmente, se precisa el establecimiento de estándares comunes en conformidad con los requisitos legales y regulatorios, como por ejemplo definir quién tiene acceso a los datos almacenados en una cadena de bloques, qué tipos de datos se almacenan, qué tipo de infraestructura se necesita para que una entidad se convierta en un nodo y quién valida estos requisitos. También requiere la definición del alcance de los contratos inteligentes, en el caso de que la solución contenga un arreglo de este tipo.

Otro de los retos organizacionales a los que se enfrenta la tecnología en el sector público es la apropiación por parte de los funcionarios. En este sentido, puede generar resistencia la implementación de una solución tecnológica que provea una mayor transparencia e inmutabilidad a las transacciones (Graglia, 2017) y reemplace en ciertos casos las acciones de los funcionarios públicos por un protocolo automatizado. Además de relegar cierta confianza en la tecnología, la lógica distribuida puede alterar dinámicas de poder y terminar con las ventajas de poder de ciertos actores (Nelson, 2018), ambos casos recurrentes en las burocracias públicas de la región.

Asimismo, los retos organizacionales dependen de los participantes que tienen acceso a la red y de los mecanismos de consenso, que no solo determinan las reglas para validar las transacciones, sino que imponen condicionalidades a los cambios futuros del esquema de gobernanza. Una solución en el sector público basada en *blockchain* deberá decidir qué organismos operarán como nodos y de qué manera se van a distribuir los roles y responsabilidades dentro del esquema; más importante aún, debe entenderse que la gobernanza diseñada deberá convivir con la que se encuentra fuera de la cadena (Pisa, 2018). Si bien la tecnología puede proveer una mayor transparencia e inmutabilidad en las transacciones, en última instancia dependerá de los funcionarios públicos encargados de subir la información al sistema y la confianza que se les tenga en el mundo analógico. A pesar de ser una tecnología basada en el consenso distribuido, la tecnología en sí misma no puede asegurar que no se reproduzcan lógicas jerárquicas o desigualdades entre participantes que existen previas a la implementación (Zambrano, 2018).

Recuadro 1

Modelos de gobernanza para una mayor colaboración y desarrollo de soluciones

Tal como se menciona a lo largo de esta publicación, los primeros casos de estudio basados en *blockchain* fueron desarrollados por compañías emergentes (*startups*) y/o gobiernos, aislados de regulaciones del sector y sistemas implementados y preexistentes. En la actualidad algunos países están comenzando a generar marcos de experimentación y colaboración entre distintos actores –academia, emprendedores, sector público, empresas, organizaciones de la sociedad civil– para fortalecer las capacidades en el diseño de soluciones, definir marcos legales sectoriales y democratizar el uso de la tecnología. Los gobiernos tienen el potencial rol de convertirse en habilitadores de este ecosistema, cocreando modelos de gobernanza para fomentar la colaboración y generando incentivos para que la red se beneficie con nuevos actores, enfoques y casos de uso.

El consorcio sin fines de lucro Alastria fue el primer caso a nivel global en desarrollar una infraestructura basada en *blockchain,* denominada Red ALASTRIA, y un estándar de identidad digital, ID ALASTRIA, para realizar transacciones con validez legal en esta red. Esta asociación cuenta a la fecha con 168 socios (Consorcio Alastria, 2018) y está construyendo una comunidad que genera estándares técnicos, provee un marco para el desarrollo de servicios comunes entre sus asociados y usuarios, y fomenta el conocimiento y el uso de la tecnología. Alastria cumple su misión a través de la mencionada plataforma colaborativa basada en una red público-permisionada; esta característica y el hecho de que no tenga una criptomoneda asociada permite eliminar el costo transaccional, de manera que el derecho a uso de la red se ofrece mediante la adhesión como socio a Alastria y el pago de una membresía. La red cuenta con un número de nodos validadores suficientemente grande como para otorgar seguridad y suficientemente pequeño como para alcanzar el consenso rápido, permitiendo una generación de bloques óptima. La Red ALASTRIA cuenta con una sólida gobernanza conformada por una Junta Directiva, un Comité de Expertos, una comisión y un equipo dedicado, estos dos últimos abocados a tareas operativas.

En la región se han comenzado a construir redes basadas en el modelo de gobernanza de Alastria, pero con una mayor participación del sector público. Por ejemplo, en 2017 la Unidad de Gobierno Digital de la Secretaría de la Función Pública (SFP) y la Coordinación de la Estrategia Digital Nacional (CEDN) del gobierno de México comenzaron a construir un proyecto de *blockchain* público con el objetivo de generar casos de uso de la tecnología para servicios digitales (CIDGE, 2017). En particular, la Red Federal de Blockchain se considera un ámbito para la generación de un

ecosistema nacional con una gobernanza colaborativa que fomente el desarrollo de aplicativos basados en el uso de *blockchain*. En este marco se realizó el lanzamiento de Blockchain HACKMX para promover la innovación digital a través del uso de nuevas tecnologías y lanzar una serie de retos públicos para desarrollar ideas en las siguientes áreas: (i) identidad digital, (ii) firma electrónica, (iii) registro público de la propiedad y (iv) certificados de depósito. Como resultado del proceso, se ha diseñado un piloto de contrataciones públicas inteligentes que fomenta la participación ciudadana y la auditoría social de las contrataciones.

En Argentina la plataforma pública abierta Blockchain Federal Argentina (BFA) tiene como objetivo integrar servicios y aplicaciones generados por el ecosistema digital argentino. Similar a la Red ALASTRIA, BFA funciona a través de una red permisionada con protocolo de prueba de autoridad realizado por nodos selladores autorizados y representativos del ecosistema. En la BFA no se almacenan archivos sino solo los *hashes* de los documentos, lo que favorece las transacciones más rápidas y delega la responsabilidad de almacenamiento a los usuarios. La gobernanza de la BFA está conformada por un Consejo de Administración, un Comité Técnico y en un futuro creará tres centros de control independiente para monitorear las partes críticas de la red.

Por último, una iniciativa reciente impulsada por el Laboratorio de Innovación del Banco Interamericano de Desarrollo (BID Lab) y con potencial de sentar bases para la colaboración regional alrededor de *blockchain* es la Alianza Global LACChain, una plataforma interoperable, abierta y colaborativa para democratizar el uso de esta tecnología y proveer servicios de calidad a poblaciones vulnerables. El objetivo de LACChain es brindar conocimiento para el desarrollo de los ecosistemas nacionales en la región, mediante el aporte de asesoría tecnológica, estímulos de mercado, estudios de viabilidad y análisis de datos para evaluar el impacto de estas iniciativas. Asimismo, LACChain aspira a convertirse en un habilitador para definir estándares y regulaciones regionales en la materia. Una de las novedades prometedoras que presenta LACChain es la elaboración de una hoja de ruta que combina el desarrollo de la infraestructura tecnológica con el marco legal necesario para resolver los problemas de gobernanza y regulación que, como se menciona en esta publicación, impiden la escalabilidad de muchas soluciones (LACChain Alliance, 2019).

Todas estas iniciativas están favoreciendo un entorno más colaborativo alrededor el uso de la tecnología *blockchain* y además ofrecen una alternativa de modelos de gobernanza que podría ayudar a que estos ecosistemas sean sostenibles a largo plazo y resilientes frente a los cambios. Cabe destacar que la mayoría de estos casos generan redes basadas en modelos públicos permisionados para favorecer entornos de prueba con reducidos costos, de fácil y rápida implementación; sin embargo, deberán ser lo suficientemente flexibles y neutrales para realizar cambios en la arquitectura ante cambios tecnológicos.

Retos tecnológicos

Los retos tecnológicos de alto nivel se vinculan a la gobernanza de la solución, al caso de uso bajo análisis y a la descentralización del almacenamiento de la información. Pasar de una solución centralizada a una descentralizada siempre implica una mayor complejidad. En el nivel más básico pasar de un sistema en el que un solo actor verifica a uno en el que muchos actores comparten esta responsabilidad requiere el uso de un protocolo de consenso, lo cual agrega demoras dependiendo de cuál se elija. Del mismo modo, pasar de un sistema en el que un tercero de confianza almacena datos en un silo centralizado a uno en el que los datos se almacenan en una red distribuida, a menudo requiere agregar capas de cifrado para establecer controles sobre quién ve la información. Adicionalmente, el alto costo de almacenar los datos de forma replicada en la cadena de bloques obligará a las organizaciones participantes a desarrollar soluciones de almacenamiento fuera de la cadena, lo que complicará aún más la forma en que se administran y aseguran los datos (Pisa, 2018).

Otro de los retos tecnológicos –y quizás el que más incide en el éxito de la implementación y sus perspectivas de escalamiento– se vincula a la **arquitectura tecnológica**. En la mayoría de casos de uso que se han pensado para el sector público, además de la cadena hay dos componentes que conforman la solución tecnológica: (i) la interfaz con los usuarios (usualmente en la web) que les permite interactuar con el sistema y (ii) una base de datos, dado que la cadena debería almacenar solamente los *hashes* que resultan de encriptar la información (Allende López, 2018) para que las transacciones se realicen de manera veloz. Es importante resaltar que para que un proceso pueda migrarse a una solución basada en *blockchain* toda la información debe estar digitalizada para que pueda ser utilizada y además los procesos deben estar automatizados. Al respecto, la interfaz de usuario es sumamente importante para democratizar el uso de la solución, por lo que se recomienda prestar especial atención al diseño, así como a las habilidades digitales y necesidades de los usuarios. Contar con una herramienta que visualice la información y permita explorarla de una manera amigable favorecerá el control de la integridad de la información.

Para que la solución que se está diseñando sea segura y tenga potencialidad de ser escalable, un tercer reto implica la necesidad de contar, entre otras cosas, con una **infraestructura de clave pública**[2] (PKI, por sus siglas en inglés)

[2] La infraestructura de clave pública es un conjunto de requisitos que permiten, entre otras cosas, la creación de firmas digitales. Cada transacción de firma digital incluye un par de claves: una privada y una pública. La clave privada no se comparte y solo la usa el firmante para firmar documentos electrónicamente. La clave pública está abiertamente disponible y es utilizada por quienes necesitan validar la firma electrónica del firmante. La infraestructura de clave pública impone requisitos adicionales, como la autoridad de certificación (*certificate authority* [CA]), un certificado digital, un *software* de inscripción de usuario final y herramientas para administrar, renovar y revocar claves y certificados (Morris, Mirkovic y O'Rourke, 2018).

que habilite transacciones criptográficas (por ejemplo, cifrado, firma digital, transacciones electrónicas). Es decir, para implementar una solución basada en *blockchain*, los gobiernos deben contar con la combinación adecuada de *hardware*, *software*, políticas y procedimientos de seguridad para realizar transacciones electrónicas de manera segura. Esta infraestructura facilita el manejo de firmas digitales en entornos donde las partes involucradas no tienen la oportunidad de verificar la autenticidad de las firmas de primera mano, otorgando confianza de que una firma digital representa a la persona que la indica. Además, una PKI puede facilitar la escalabilidad de la solución, ya que cuantas más partes estén involucradas en una red es más probable que las partes no conozcan o no confíen en las firmas digitales de los demás. A pesar de esto, una PKI tradicional introduce elementos de intermediarios (las autoridades de certificación y registración), para lo cual están surgiendo modelos descentralizados (*decentralized public key infrastructure* [DPKI]) que intentan resolver esta cuestión. De todas formas, vale destacar que las *blockchain* permisionadas como la BFA funcionarán como una PKI, ya que hay una autoridad de registro centralizada y una de certificación descentralizada.Otro reto relacionado son el **volumen y el tipo de datos** que se almacenan en la cadena. La tecnología *blockchain* actualmente no tiene capacidad para almacenar grandes volúmenes de datos[3] debido al alto costo de replicación a múltiples nodos y su consecuente sincronización. Por este motivo se recomienda almacenar datos no transaccionales –sobre todo si se trata de información personal– en una base de datos separada y solamente almacenar los *hashes* de estos datos en la cadena de bloques. Si bien esta arquitectura asegura la integridad y seguridad de los datos originales, se limita una de las características fundamentales de la tecnología *blockchain*: la distribución de los datos (que en este caso son almacenados en una base de datos separada) y su verificabilidad (solamente los valores *hash* están almacenados en la cadena de bloques por lo que la verificación de la integridad de los datos originales requiere consultar la base de datos). En cuanto al tipo de datos que formarán parte de la solución, se recomienda no subir aquellos que atenten contra la privacidad de las personas[4] o

[3] Como la tecnología *blockchain* está diseñada para retener todas las transacciones previas, el volumen de almacenamiento aumentará con el tiempo y deberá pronosticarse en función de las demandas de la red y la cantidad de transacciones proyectadas.

[4] En la actualidad se discute si un dato personal *hasheado* puede ser considerado como un dato personal (UE, 2018b) y, como consecuencia, sujeto a regulaciones (por ejemplo, mediante la General Data Protection Regulation en el caso de la Unión Europea [UE]). En la actualidad no hay pruebas matemáticas concluyentes de que un *hash* pueda ser irreversible; por ejemplo, a través de las técnicas de computación cuántica actualmente disponibles aún no se pueden revertir (Allende López, 2019). Sin embargo, se deben tomar los recaudos necesarios por si esta situación cambiara en el futuro.

tengan el potencial de ser borrados o editados, ya que si bien los protocolos de encriptación usados actualmente son bastante robustos, con el tiempo pueden llegar a ser vulnerados.[5]

Además, existe un desafío vinculado al consumo de **procesamiento computacional y energético de la tecnología** en las redes públicas con determinados protocolos de consenso. Para fomentar la competición por el minado de bloques –que consiste en encontrar el código que concatenado a la data del bloque da como resultado un *hash* válido– que garantiza la seguridad de la cadena, se han desarrollado varios mecanismos de consenso que recompensan con criptomoneda al ganador de esa competición para cada bloque. Algunos de estos, como el llamado prueba de trabajo (PoW, por sus siglas en inglés), que actualmente es el más conocido por su uso en la criptomoneda Bitcoin y en la plataforma Ethereum, incitan a los "mineros" a emplear altos volúmenes de procesamiento computacional, lo que acarrea un consumo muy elevado de energía.

A nivel de ***software***, los retos tecnológicos consisten en conseguir que las redes sean capaces de procesar un mayor número de transacciones por segundo, que el permisionado de nuevos nodos y el funcionamiento de los canales privados en las redes público-permisionadas sean más eficientes y que redes diferentes sean interoperables. Sin embargo, alcanzar este objetivo no es tan fácil porque diferentes redes tienen distintos protocolos de consenso, y actualmente no hay un estándar para intercambiar datos entre las diferentes cadenas de bloques.

Retos regulatorios

Pasar de modelos centralizados a descentralizados también implica considerar retos legales y regulatorios. Si el marco legal de un gobierno tiene requisitos específicos sobre el uso de intermediarios o socios confiables, puede ser complicado utilizar una solución basada en la tecnología *blockchain*, o bien esa solución no podrá ser escalable. En casos de uso donde la regulación desempeña un papel importante, puede ser necesario incluir reguladores en el diseño del proyecto y proporcionar medios para que estos puedan garantizar el cumplimiento de las leyes. Al respecto, ACT-IAC (2018) recomienda revisar las regulaciones específicas al caso de uso (por ejemplo, regulaciones en materia de identidad digital).

[5] Véase por ejemplo: *https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/*.

Como se ha mencionado anteriormente, las instituciones interesadas en utilizar la tecnología deben determinar cómo pueden cumplir con las leyes **de privacidad y seguridad de datos** existentes. En cuanto a la privacidad, es importante considerar que los datos que van a ser almacenados en la cadena de bloques pueden estar a disposición para todos los participantes de la red. Si bien en la actualidad no hay pruebas definitivas de que la información *hasheada* se pueda revertir, deben tomarse los recaudos necesarios en los casos en que se trabaje con datos sensibles como información personal de ciudadanos o vinculados a la seguridad pública.[6]

Un asunto vinculado a la privacidad es el del ingreso de datos sensibles, clasificados, falsos o incorrectos a una cadena de manera inapropiada o ilegal. La tecnología *blockchain* funciona según el principio basura dentro, basura fuera (*garbage in, garbage out*); esto es: si alguien (por ejemplo, un oficial público) carga una información falsa o incorrecta en una cadena de bloques (ya sea por descuido o engaño) la información seguirá siendo falsa (Pisa y Juden, 2017). La verificación de los datos de forma automática por los nodos está limitada a reglas predeterminadas en el diseño de la arquitectura de la solución. Si no hay reglas y/o protocolos para detectar el ingreso de datos falsos o si la detección es un ejercicio complejo, la tecnología no podría ser capaz de impedir su almacenamiento, ni sería posible su corrección o eliminación.[7] Para prevenir tales incidentes, el diseño de una buena gobernanza es crítico.

Otro reto regulatorio está vinculado al **derecho al olvido**. La inmutabilidad de los datos almacenados en la cadena de bloques podría restringir este derecho a pesar de que ya está asegurado legalmente en muchos países. En la actualidad, con las implementaciones disponibles no hay posibilidad de modificar o borrar los datos almacenados en la cadena de bloques, lo que hace que la tecnología *blockchain* (sobre todo la pública) no sea viable para datos sensibles amparados bajo la jurisdicción del derecho al olvido. Con relación a la inmutabi-

[6] Como se ha mencionado, una posibilidad para proteger los datos sensibles, pero en detrimento de ciertas características de la tecnología (distribución y la verificación), puede ser ocultarlos de la vista de los participantes a través de su almacenamiento en una base de datos separada y archivar valores *hash* en la cadena de bloques. Bajo esta premisa, dado que la función *hash* solamente funciona en una dirección, esta arquitectura permite asegurar la integridad de los datos originales y protegerlos contra el acceso de los participantes de la red de *blockchain*. No obstante, existen especialistas que sostienen que, bajo ciertos parámetros y con una suficiente capacidad computacional, se podría derivar información a partir de un *hash* a través de múltiples intentos de prueba y error, y por lo tanto el *hash* debería considerarse una extensión de la información personal.

[7] Cabe destacar que existen algunos experimentos con reglas de gobernanza que en casos específicos permiten la modificación de la cadena de bloques posteriormente.

lidad de los datos, otro reto se vincula al derecho de rectificar información de las personas que se encuentra en manos del gobierno. Si bien dicha corrección puede realizarse, el hecho de que quede plasmado en la cadena de bloques puede vulnerar el derecho a la privacidad, por lo cual deben tomarse recaudos para revisar la información que ingresa y los casos en los que puede modificarse.

Los tomadores de decisión en algunos casos deberán considerar la modificación de las leyes existentes para facilitar el uso de modelos descentralizados (Pisa, 2018). Adicionalmente, existe un desafío vinculado a la **jurisdicción** pertinente. Por su atributo de distribución de la información, *blockchain* tiene la capacidad de cruzar fronteras jurisdiccionales ya que los nodos de una cadena de bloques se pueden ubicar en cualquier parte del mundo. Esto puede plantear una serie de cuestiones jurisdiccionales complejas que requieren una consideración cuidadosa respecto de las relaciones contractuales relevantes en un entorno descentralizado (DLA Piper, 2017). Iniciativas como Alastria en España, la Red Federal Argentina o las redes que vienen siendo promovidas por el BID Lab bajo la iniciativa LAC-Chain podrían reducir este problema si se restringen algunas redes a nodos que estén situados en el mismo territorio geográfico. En caso de que dichas redes contengan más de una jurisdicción territorial, se recomienda realizar un diagnóstico jurídico para comprobar que este tipo de modelos descentralizados son viables.

En cuanto a la **exigibilidad legal de los contratos inteligentes**, su uso también plantea importantes cuestiones legales en relación con la regulación aplicable. Dado que los contratos inteligentes son códigos informáticos predefinidos, su uso puede generar problemas de exigibilidad legal si se intenta analizarlos dentro de la definición tradicional. Si bien el objetivo de estos programas escritos en las cadenas de bloques es no depender de una autoridad central, es posible que alguna de las partes solicite la participación de un árbitro para resolver alguna disputa no contemplada en un contrato que se ejecuta automáticamente. Una recomendación a la hora de implementar una solución que incluya contratos inteligentes es asegurar una disposición de resolución de disputas y un mecanismo asociado para reducir la incertidumbre (DLA Piper, 2017). Sin embargo, esto desarma el propósito inicial del uso de contratos inteligentes,[8] por lo que su utilidad en algunos entornos puede ser discutida.

Un reto vinculado al anterior viene dado por la eliminación de intermediarios, que en ciertos casos han servido como implementadores de salvaguardas regu-

[8] Otro gran beneficio de los contratos inteligentes es la agilidad de constatación y la ejecución de acciones vinculadas a dichas constataciones. Estos beneficios permanecen incluso con la inclusión fuera de línea (*offline*) de una estructura de arbitraje.

latorias. En este sentido, se plantea el desafío de implementar cambios sistémicos más amplios cuando sea necesario el cumplimiento de normativa regulatoria adicional (Morris, Mirkovic y O'Rourke, 2018). Cabe señalar, en principio, que los mismos contratos inteligentes podrían encargarse de la verificación del cumplimiento de esta normativa.

Por último, existe el reto regulatorio vinculado a la función de notarización de los registros; para que *blockchain* pueda funcionar como un notariado digital, debe existir una regulación que lo habilite. Si bien algunos marcos legales se adecuaron para aceptar la notarización,[9] se necesita avanzar en este sentido dado que esta función se vincula con varias de las aplicaciones de la tecnología en el sector público.

Retos de talento

Otro de los retos de implementación es el **de generación de talento y conocimiento (*expertise*)** en esta tecnología dentro del sector público. Si bien la implementación de pilotos ha estado hasta ahora a cargo del sector privado, organizaciones de la sociedad civil o laboratorios de innovación en el sector público es necesario introducir conocimiento y perfiles específicos en temas de innovación tecnológica en las instituciones que desean implementar (y escalar) una solución basada en *blockchain* para una clara identificación del problema, el análisis de los riesgos y debilidades de la solución y los retos de escalarla.

El hecho de que la gobernabilidad del sistema se dé a través del consenso algorítmico le presenta al sector público el desafío de generar capacidades para entender el código, poder rendir cuentas de los resultados de la solución (Berryhill, Bourgery y Hanson, 2018) y establecer los principios (que luego se convertirán en código) que automatizan las decisiones de las personas. Por ende, además de conocer el contexto de dicho código, se necesita poder leerlo, comprenderlo y eventualmente auditarlo. Existen ya muchas historias en las que la falta de una auditoría del código o de los procesos *offline* ha producido pérdidas millonarias. Generar capacidades al interior del sector público es clave para monitorear desigualdades y jerarquías emergentes entre los miembros de la red en conocimientos en minería, desarrollo de soluciones y código, entre otros (Zambrano, 2018).

Retos de uso y generación del ecosistema

Un reto vinculado al anterior está dado por el uso de la tecnología por parte de los distintos actores del ecosistema digital. Muchos de los proyectos piloto generados en la actualidad están liderados por grupos de emprendedores y *startups* altamente calificadas, tienen una escala moderada, pocos beneficiarios y carecen de una estrategia a

[9] En algunos casos existe un vacío en la regulación de firma digital que habilita el uso de *blockchain* para notarizar registros.

largo plazo (Zambrano, 2018). En este contexto deben generarse capacidades para democratizar su uso y experimentación. Este es un claro desafío para los países de la región –y sobre todo en el caso de pilotos que beneficien a poblaciones vulnerables– si se tiene en cuenta que el desarrollo de este tipo de soluciones implica tener conocimiento del uso de herramientas tecnológicas así como del manejo de claves públicas y privadas. Además de generar habilidades digitales y centrarse en un adecuado diseño de servicios basado en la necesidad de los usuarios, a la hora de implementar una solución basada en tecnología *blockchain* se pueden identificar organizaciones de la sociedad civil u otros actores que apoyen la utilización de estas herramientas.

Otro desafío vinculado al uso de la tecnología se relaciona con la experiencia de los usuarios. Tal como se mencionó anteriormente, el desarrollo de una interfaz amigable y/o herramientas de visualización para que las personas puedan explorar los datos y corroborar la integridad de los mismos son clave para la democratización de la tecnología.

Asimismo, el sector público puede convertirse en un habilitador para generar un ecosistema[10] y fomentar la innovación alrededor del diseño de soluciones basadas en tecnología *blockchain*. Los gobiernos desempeñan un rol en el establecimiento de estándares, la revisión de la regulación para permitir el uso de modelos descentralizados y nuevas tecnologías, y la reducción de barreras a la entrada para democratizar el uso de esta tecnología, sobre todo en soluciones que permitan resolver problemas públicos.

1.2.2. Checklist *de condiciones habilitantes*

En función de lo anterior, este apartado detalla algunas condiciones habilitantes que hacen que una solución basada en *blockchain* tenga probabilidad de ser escalable y sostenible. Si bien los detalles de la implementación y el problema a resolver son clave para el éxito de la solución, existen ciertas cuestiones que favorecen la implementación.

Marco legal para modelos descentralizados

Como se ha mencionado, para que un piloto pueda tener potencial de ser escalable, se necesita contar con un marco legal que habilite los modelos descentralizados y la validez de compartir información –no sensible y que no atente contra la privacidad de la persona– con otros miembros de la red que no pertenecen al sector público. De acuerdo con McKinsey (2018), uno de los problemas que enfrenta la escalabilidad de las soluciones basadas en la tecnología *blockchain* es la falta de estándares comunes; en este sentido, los gobiernos pueden desempeñar un rol dominante

[10] Un artículo que detalla los actores del ecosistema de *blockchain* puede leerse en: http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf.

ya que en determinados casos de uso (por ejemplo, registros públicos) tienen total responsabilidad para definir la regulación y podrían, por tanto, exigir un estándar específico.[11]

Digitalización de los registros

Una de las principales condiciones habilitantes es la existencia de activos digitales que puedan ser equivalentes al papel en el mundo digital (WEF, 2018). Si bien como parte de algunos pilotos de *blockchain* se han digitalizado archivos, lo que constituye un incentivo positivo para la modernización, para asegurar la inmutabilidad de las transacciones debe existir certeza jurídica de que estos no podrán modificarse en el mundo analógico, para lo cual la digitalización y automatización de los procesos son clave. Adicionalmente, debe asegurarse que sea posible crear un registro permanente del activo para que pueda ser almacenado en la cadena.

Tipos de datos a almacenar

Blockchain no es una solución viable cuando la información que debe almacenarse en la cadena es sensible y/o está regulada por políticas de privacidad de los datos. Sin embargo, si la información que se almacena en la cadena puede convertirse en registros de transacciones en lugar de información personal (por ejemplo, en los modelos de identidad soberana que se mencionan en la segunda parte), *blockchain* puede ser utilizado (WEF, 2018).

Dado que *blockchain* asegura la inmutabilidad e integridad de la información que es parte de la cadena, tampoco se recomienda utilizar esta tecnología en casos donde los datos deban eliminarse o modificarse. Por último, tampoco es recomendable subir grandes volúmenes de datos dado que en la actualidad *blockchain* tiene una capacidad limitada –de hecho, en los casos de redes públicas el tamaño de cada bloque está predeterminado– para almacenar información.

Costos transaccionales

En la actualidad, una *blockchain* pública es una solución viable para aquellos casos donde no se requiera transacciones en tiempo real. La velocidad de procesamiento se ve comprometida a medida que se incrementan los bloques o cuanto mayor tamaño tengan, por lo que se recomienda analizar la información que formará parte de la cadena de bloques. Como solución muchos desarrollos almacenan la información en sistemas complementarios a la cadena de bloques y solo alojan allí los *hashes* de la información. Otras variables a tener en cuenta si se opta por una red pública es el costo de las transacciones, la necesidad (o no) de anonimato de los nodos y la privacidad de la información.

[11] Esta es una de las novedades que presenta el programa LACChain liderado por el BID Lab con respecto a otras iniciativas que solo se centran en la infraestructura tecnológica; en él se incluye la propuesta de un marco legal y de gobernanza que complemente la infraestructura tecnológica.

1.3
Hoja de ruta para el diseño de una solución

A lo largo de la publicación se puede observar que, bajo ciertas condiciones, la tecnología *blockchain* puede agregar valor para resolver problemas del sector público. Dado que esta tecnología podría habilitar el diseño de una lógica distribuida y descentralizada en la provisión de servicios públicos (Zambrano, 2018), algunas funciones del gobierno –por ejemplo: registrar transacciones, validar información y/o verificar el cumplimiento de normas– pueden incluso ser reemplazadas por la tecnología.

Sin embargo, esto no significa que la tecnología *blockchain* es la solución a todos los problemas de la administración pública. Hay que tener en cuenta, por más obvio que parezca, que la solución es la que debe ajustarse al problema y no al revés. Entonces, la guía general que se ofrece a continuación, si bien se centra en la tecnología *blockchain* empieza con el entendimiento del problema.[12] Los pasos siguientes asumen que luego de este primer paso se ha concluido que la tecnología *blockchain* es una opción por considerar. Independientemente de la tecnología que se pretenda utilizar, se recomienda consultar los Principios Digitales,[13] recientemente adoptados por el Banco Interamericano de Desarrollo (BID), como una guía general del uso de tecnología en proyectos de desarrollo.

[12] Actualmente muchas organizaciones están comenzando a documentar los pasos necesarios para implementar una solución basada en *blockchain* (ACT-IAC, 2018; AGESIC, 2018). Por ejemplo, el *Playbook* para funcionarios de gobierno de ACT-IAC (2018) define cinco fases de implementación: (i) diagnóstico del problema, (ii) preparación organizacional, (iii) selección de la tecnología, (iv) implementación e (v) integración de la solución.

[13] Más información disponible en: *https://digitalprinciples.org/.*

1.3.1 PASO I · Entender el problema

El primer paso para prototipar y/o diseñar una solución consiste en entender el problema que se intenta resolver. Si bien esto parece una tarea simple, en la práctica existen muchos intentos que fracasan por una falta de entendimiento del problema que se quiere resolver. En muchas instancias se pone más énfasis en una solución preseleccionada, lo cual no siempre funciona. Entonces, tener una clara definición del problema ayudará a decidir más adelante si *blockchain* es la mejor solución para resolverlo o si se necesitan otras tecnologías alternativas o complementarias para abordarlo.

En este paso se propone utilizar el test incluido en el apartado 1.1, que fue elaborado para entender si *blockchain* es una tecnología a considerar. En general, es más probable que *blockchain* sea una solución pertinente si: (i) en el problema intervienen múltiples partes que no confían entre sí; (ii) se requiere contar con un registro histórico de la información vinculada al problema y de las transacciones; (iii) la información de las transacciones debe ser validada a través del consenso algorítmico y no se necesita que esta validación sea en tiempo real; y (iv) se puede (o se debe) prescindir de intermediarios para resolver el problema. Si se considera que *blockchain* puede efectivamente ser una opción se puede continuar con el resto de esta guía.

1.3.2. PASO II · Analizar el contexto del problema

Luego de definir con claridad el problema, se recomienda analizar su contexto. Para ello, se requiere comprender el proceso detrás del caso de uso y las transacciones involucradas. Para el caso particular de la tecnología *blockchain*, es preciso identificar aquellas instancias en las cuales existe una falta de confianza y/o se necesita incrementar la transparencia. Lo importante en este paso es analizar cuáles son los atributos de la tecnología que contribuyen a resolver el problema, y si se necesitan sumar otras tecnologías (por ejemplo, inteligencia artificial [IA], Internet de las cosas [IoT, por sus siglas en inglés], entre otros) para optimizar su uso.

Adicionalmente, entender la regulación y jurisprudencia también es importante para la sostenibilidad de la solución. El marco legal y organizacional puede afectar su alcance; por ejemplo, si están agregándose actores no identificados en el marco legal que ampara el proceso en cuestión se corre el riesgo de que la solución no sea escalable, al menos en el corto plazo.

1.3.3. PASO III · Mapear los actores

Como siguiente paso, se recomienda identificar los perfiles de usuarios, actuales y potenciales, que formarán parte de la solución. Además del tipo de actor (sector público, academia, sociedad civil, etc.), entender sus intereses e incentivos es importante a la hora de diseñar una solución basada en *blockchain* ya que ayudará a definir las características de la red y los permisos a ser asignados en caso de que se opte por una solución de tipo privada y/o permisionada. Tal como se menciona en la tercera parte de esta publicación, la tecnología puede contribuir a generar confianza y acuerdos entre usuarios en entornos complejos, y sobre todo cuando estos tienen intereses dispersos (Allende López, 2018). El diseño de los nodos, sus permisos y transacciones es importante para generar valor agregado.

También deben analizarse las transacciones que van a ser parte de la solución, el rol de los participantes en cada una de ellas –si van a interactuar con la red a través de una interfaz web, si mantiene una copia de la cadena, etc.– y los permisos necesarios para estos actores. Cabe destacar que cuanto más diferentes sean los participantes de esta red, se necesitarán consensos más complejos (Allende López, 2018).

1.3.4 PASO IV · Diseñar la arquitectura de la solución a través de un prototipo rápido que pueda ser escalado

Una vez analizado el problema y las características de los participantes potenciales, el siguiente paso consiste en comenzar a diseñar la arquitectura de la solución. En esta etapa, de acuerdo con ACT-IAC (2018), para el caso de la tecnología *blockchain* se recomienda comenzar prototipando la solución, de manera tal de poder evaluar sus resultados y corregir con base en lo aprendido en la prueba de concepto.

Tal como se mencionó previamente, el diseño de la arquitectura implica no solo elegir el tipo de red, sino construir –en caso de que no existan– los sistemas complementarios a la cadena de bloques (interfaces, herramientas web, interfaces de programación de aplicaciones [API, por sus siglas en inglés], bases de datos). En este sentido, Verhulst (2018) recomienda a los gobiernos no realizar contratos restrictivos con proveedores, sino asegurar la interoperabilidad de los diferentes sistemas y el desarrollo de estándares técnicos abiertos. Por otra parte, a la hora de realizar un proceso de contratación para

la solución ACT-IAC (2018) aconseja comenzar con un proceso pequeño para contratar el piloto, de manera de no quedar cautivo en un proceso largo y burocrático sin antes evaluar la viabilidad de la solución, y poner especificaciones técnicas poco restrictivas, de manera tal de tener flexibilidad ante cambios en la tecnología que puedan aportar a la solución.

Asimismo, se necesita decidir el tipo y las características principales de la red. Tal como se menciona en la segunda parte de la publicación, la mayoría de los casos de uso en el sector público utilizan redes públicas permisionadas o redes privadas.[14]

En la actualidad muchos gobiernos están construyendo su propia infraestructura para fomentar el desarrollo de soluciones basadas en *blockchain* en el sector público (por ejemplo, la Red Federal en Argentina). Si bien esta puede ser una opción para montar la arquitectura, deben revisarse las características de la red y compararlas con los nuevos desarrollos de la tecnología para definir si cubre las necesidades de la institución (UE, 2018a). Al respecto, la UE (2018a) menciona otra opción para tener en cuenta y es la de *Blockchain Platform as a Service*, la cual provee una infraestructura compartida que aloja protocolos, herramientas y provee un entorno para el desarrollo de pruebas. De esta manera, se tiene una caja de arena (*sandbox*) para el prototipado rápido (y en algunos casos menos costoso) de soluciones.

Otro aspecto importante en el diseño de la arquitectura es la creación de herramientas de visualización de la información generada. La interfaz de usuario es sumamente importante para democratizar el uso de la solución, por lo que se recomienda prestar especial atención a los usuarios. Contar con una interfaz amigable que permita verificar la integridad de la información permitirá democratizar el uso de la tecnología, para lo cual se sugiere poner especial atención a su diseño y al costo asociado de su desarrollo.

Por último, se recomienda analizar los sistemas y arquitecturas paralelas que se están utilizando en la actualidad y evaluar su continuidad bajo la nueva solución (por ejemplo, bases de datos, API, protocolos y estándares de la información). De esta manera, la arquitectura tendrá mayores posibilidades de ser compatible con los sistemas actuales, generando menos problemas a la hora de reemplazarlos o complementarlos y facilitando su escalabilidad.

[14] Para revisar los tipos de red existentes y sus características, se recomienda ir a la tercera parte de esta publicación.

1.3.5. PASO V · Definir la gobernanza

Un paso clave para la sostenibilidad de la solución es diseñar reglas de juego claras, transparentes y que aseguren la responsabilidad y participación del ecosistema (Verlhust, 2018). En esta instancia se requiere comenzar a diseñar la gobernanza en coordinación con los actores de la red, definiendo roles, responsabilidades, reglas de entrada de nuevos participantes, incentivos y principios, entre otros. Esta gobernanza deberá respetar las regulaciones vigentes para el caso de uso, de manera tal de favorecer su escalabilidad desde el punto de vista del marco legal.

En algunos casos la solución puede diseñarse en alguna red existente, con un modelo de gobernanza ya definido. Para conocer algunos modelos de gobernanza vigentes y sus características, se recomienda volver a revisar el apartado sobre retos organizacionales y de gobernanza que se encuentra previamente en esta primera parte de la publicación.

1.3.6. PASO VI · Evaluar el prototipo

El paso más importante del diseño de una solución es evaluar si resuelve el problema identificado. En esta instancia se recomienda realizar una evaluación rigurosa en la fase de prototipado, recogiendo el *feedback* de los usuarios de la red e identificando las principales lecciones aprendidas.

La evaluación del prototipo puede arrojar alguno de estos resultados: (i) si la prueba de concepto logra resolver el problema identificado se escala la solución; (ii) se puede iterar una nueva solución que corrige la arquitectura en función de las lecciones aprendidas; (iii) se puede explorar una tecnología alternativa para lograr resolver el problema.

II

Usos potenciales de *blockchain*

Esta parte explora los usos potenciales de la tecnología *blockchain*. Para ello, se empezará revisando el valor agregado de sus atributos particulares para resolver problemas del sector público. Tal como se verá más adelante, para que la tecnología genere valor agregado es importante entender el problema que se quiere resolver y luego prestar especial atención al diseño de la solución. Para cada categorización de valor agregado, se presentarán casos de uso sectoriales y ejemplos de implementación. Los ejemplos presentados han tenido desafíos de implementación particulares, que vale la pena analizar ya que reflejan características del sector público de la región que deberán atenderse antes de comenzar a diseñar la solución (por ejemplo, la falta de digitalización y automatización de procesos, la estandarización de la información, la definición de usuarios y ecosistema de uso, etcétera.).

Hay dos grandes motivos por los que es importante prestar atención a los usos potenciales de *blockchain*. En primer lugar, es importante entender las implicancias de su uso para poder *regular* (o, si fuera el caso, *desregular*) los distintos ámbitos en los que podría aplicarse. Por ejemplo, como se menciona en la primera parte, en algunos países el cumplimiento del derecho al olvido[15] puede determinar qué tipo de información se puede o no incluir en cada bloque, ya que cualquier dato que se registre en una cadena pública será imposible de borrar. Adicionalmente, para poder montar sistemas de identidad sobre *blockchain*, las entidades participantes deberán reconocer los certificados digitales inscritos y escritos en la cadena como jurídicamente válidos. Más aún, la legislación relacionada a firmas digitales o a privacidad de la información también puede afectar el uso de esta tecnología.

En general, se debe adoptar una postura que promueva la innovación y la mayor eficiencia de procesos, especialmente en el sector privado, pero siempre velando por la integridad y privacidad de la información personal. En aquellos casos en los que ambos objetivos se contrapongan, el funcionario público deberá evaluar los cambios que puedan requerirse para balancearlos de manera efectiva. Esta evaluación requiere un buen entendimiento de la tecnología.

En segundo lugar, es importante que los funcionarios públicos entiendan la tecnología para poder reconocer los distintos tipos de *blockchain*, sus atributos y los diferentes usos que puede tener. Esto permitirá una mejor evaluación de la tecnología y la identificación del tipo de problemas que puede contribuir a resolver. Para ayudar en esta labor se considera importante entender el potencial *valor agregado* que *blockchain* aporta a los distintos ámbitos del sector público.

[15] Se refiere a la posibilidad de que, frente a la solicitud de la parte, se bloquee o borre información que, aunque sea cierta, se considera que afecta el honor, la imagen o la intimidad de alguien.

2.1.
Generar valor agregado para el sector público

Teniendo en cuenta las iniciativas que están siendo exploradas en el sector público en la región y en función de los atributos de la tecnología,[16] pueden identificarse cuatro grandes categorías en donde podría pensarse que una tecnología como *blockchain* podría ser de utilidad para el sector público: (i) desintermediación de la información, (ii) tokenización de activos, (iii) automatización de procesos e (iv) interoperabilidad en el borde.

2.1.1. Desintermediación de la información

En muchas instancias la generación de información en el sector público se basa en una cadena de procesos compuesta por distintas personas o entidades. A través de la tecnología, la información puede registrarse de manera segura y confiable, convirtiendo a la red en una especie de notariado digital de datos y transacciones. Potencialmente, el incluir estos procesos en una cadena de *blockchain* permitirá prescindir de algunos de estos intermediarios, aumentar la trazabilidad de cada etapa del proceso de manera confiable y reducir costos tanto en tiempo como en recursos.

2.1.2. Tokenización de activos

El uso de la tecnología puede permitir expresar distintos activos como fichas (*tokens)*, de manera que se los pueda representar de manera digital y así contar con un registro confiable de los cambios de propiedad (o de localización, en el caso de cadenas de producción o de distribución). Esta característica también permite la posibilidad de atomizar la propiedad de un solo activo entre muchos propietarios, como se explica más adelante.

[16] La tercera parte explica brevemente cómo funciona la tecnología y lista sus principales atributos.

2.1.3. Automatización de procesos

Una ventaja de la inscripción de contratos inteligentes en un registro distribuido es la posibilidad de automatizar procesos a través del establecimiento de reglas que deberán cumplirse para que se realice cierta acción (ejecución del contrato) de manera automática sin intermediarios de confianza. El pago automático de transferencias condicionadas cuando se cumplen condicionalidades predefinidas, el cobro de bienes y servicios después de haber sido entregados o el hacer cumplir diversas regulaciones pueden traducirse en reglas incluidas en contratos inteligentes.

2.1.4. Interoperabilidad en el borde

Uno de los principales retos para la prestación integrada de servicios de gobierno es la necesidad de conectar los distintos sistemas de las entidades públicas y privadas de forma segura y confiable. El uso de *blockchain* para la certificación de información ciudadana puede permitir que sean los mismos ciudadanos los que ayuden a que los distintos sistemas operen entre sí sin la necesidad de que estén integrados, otorgando en tiempo real los permisos necesarios para que su información personal pueda ser accedida por distintas entidades. Este enfoque tiene además la ventaja de permitir una mayor trazabilidad en el acceso de información personal del ciudadano.

Es importante notar que estas categorías no representan beneficios *exclusivos* de la tecnología. Para ilustrar mejor el potencial valor agregado de *blockchain* en estos casos, se han recogido algunos casos de uso[17] entre las cuatro categorías, los cuales se listan en el cuadro 1. Para cada caso se analizan las características de la tecnología que la convierten en una opción a considerar, se discuten brevemente otras tecnologías capaces de generar resultados similares y se repasan los supuestos que deben cumplirse en cada caso para poder implementar una solución basada en *blockchain*.

[17] La lista de casos de uso analizada no es de ninguna manera exhaustiva. Sin embargo, se considera que representan la gama de opciones de uso de la tecnología.

CUADRO 1. CASOS DE USO ANALIZADOS

TIPO	CASOS DE USO	EJEMPLO
Desintermediación de la información	Incrementar la transparencia de los procesos	Subsidios a artistas en Bahía Blanca (Argentina)
	Facilitar la auditoría de información	Piloto para compras públicas (México)
	Asegurar la integridad de los datos	Registro de propiedad de tierras (Georgia)
Tokenización de activos	Propiedad intelectual	Obras de arte
Automatización de procesos	Facilitar la automatización de los procesos públicos	Administración General de Servicios (GSA, por sus siglas en inglés, Estados Unidos)
Interoperabilidad en el borde	Generar credenciales digitales	Certificados educativos (Bahamas)
	Construir una identidad soberana	Barrio 31 (Argentina)

2.2.
Incrementar la transparencia de los procesos

Blockchain tiene el potencial de facilitar el registro y la publicación de datos y procesos públicos, prescindiendo de intermediarios que puedan manipular o retrasar el procedimiento y fomentando su monitoreo por parte de la ciudadanía. Los elementos intrínsecos de la tecnología que facilitan este objetivo son la distribución de la información, la disponibilidad de los datos en múltiples nodos que pueden estar fuera de la administración pública y la posibilidad de verificación de la integridad de la información por parte de cada uno de ellos.[18] Por ejemplo, a través de la implementación de contratos inteligentes pueden asignarse subsidios de manera más transparente y eficiente.

En el momento en que alguien comienza a realizar transacciones en el sistema se origina un historial de todas las interacciones y transacciones que está disponible para todos los participantes, lo cual genera un alto nivel de transparencia, trazabilidad y confianza en la integridad de la red. Adicionalmente, la tecnología habilita la notarización de la información, es decir, puede certificar que determinada información no ha sido alterada.

Si bien una red privada distribuida puede agregar restricciones sobre quién puede escribir o leer transacciones, conserva la característica de acceso común a su conjunto de transacciones. Por otro lado, cuanto más distribuidos se encuentren los nodos, no solo dentro de las organizaciones de la administración pública con competencia en el proceso o con roles de auditoría sino en organizaciones fuera de la administración pública, la solución tendrá mayor probabilidad de incrementar la transparencia e integridad de la información.

[18] Como se menciona a lo largo de la publicación, en el caso de una *blockchain* privada y/o permisionada se debilita el grado de dificultad para cambiar información en la cadena.

2.2.1. Asignación de subsidios públicos a artistas: el caso del municipio de Bahía Blanca

El municipio de Bahía Blanca, perteneciente a la provincia de Buenos Aires en Argentina, ha creado en el año 2007 el Fondo Municipal de las Artes, el cual otorga subsidios a artistas locales. El monto del fondo y la cantidad de subsidios varían de manera anual y su otorgamiento no tiene un criterio único, aunque intenta mantener un balance en la asignación de acuerdo con las distintas disciplinas artísticas (Cepeda et al., 2017). Un consejo consultivo conformado por el director del Instituto Cultural de Bahía Blanca, representantes de los sectores de las artes y un representante de los empleados del instituto realiza la selección de los proyectos.

El caso de Bahía Blanca ha sido uno de los primeros pilotos a nivel local y fue desarrollado con la finalidad de experimentar la tecnología *blockchain* en el sector público, aprender de las particularidades de la tecnología y demostrar que puede utilizarse como un "notariado digital" de información pública (Cepeda et al., 2017). El problema central que buscó resolver el piloto es incrementar la transparencia en la asignación de subsidios públicos del Fondo de las Artes del Instituto Cultural de Bahía Blanca, y de este modo aumentar la confianza de la ciudadanía en el proceso. A través del atributo de inmutabilidad de los registros que otorga la tecnología *blockchain*, la información sobre el otorgamiento de subsidios (por ejemplo, destinatarios, montos, fecha de adjudicación, entre otros) no podrá ser alterada por funcionarios sin dejar un registro de la acción.

Descripción de la solución

La solución ha sido desarrollada en una red pública (Ethereum) y se ha diseñado una interfaz para que cualquier usuario con acceso a la red pueda corroborar que la información sobre el proceso de asignación no ha sido alterada por ningún funcionario público municipal.

La implementación ha sido desarrollada por técnicos no pertenecientes al municipio y tuvo una duración de tres meses; el lanzamiento oficial se realizó en noviembre de 2017. Como paso previo al piloto se digitalizó toda la información vinculada al otorgamiento de subsidios del mencionado fondo.

El piloto emite tres certificados de confianza bajo la tecnología *blockchain*. El primero de ellos está vinculado a la asignación del subsidio al artista local con todos sus datos, el segundo se realiza al momento del otorgamiento del subsidio, con base en la información de gastos que realiza el artista y de acuerdo con la regulación del fondo. Finalmente, un tercer certificado se emite con base en la información analizada por el Instituto Cultural, el cual verifica

si la información emitida por el adjudicatario cumple con las condicionalidades del subsidio y certifica la finalización de la obra.

Tecnologías alternativas

Es importante mencionar que hay otras tecnologías que permiten compartir datos sobre los procesos de manera transparente. Por ejemplo, una base de datos tradicional (sea centralizada o distribuida) con protocolos particulares para asegurar su seguridad también permite autorizar el acceso de lectura a organizaciones fuera de la administración pública. El valor particular de una *blockchain* pública es que los participantes pueden tener mayor confianza en que los datos almacenados en la cadena de bloques no han sido manipulados desde su ingreso; y en caso de que lo fueran, es posible rastrear los cambios.

Condiciones para implementar esta solución con tecnología blockchain

Este caso demuestra que la implementación de un piloto basado en la tecnología *blockchain* necesita de ciertas condiciones tecnológicas para ser implementado, y de hecho puede servir como incentivo para comenzar con procesos de modernización en el sector público. La evaluación del piloto resalta que *blockchain* requiere de una estrategia de gobierno digital que implique la digitalización de los procesos, la existencia de firma electrónica y la infraestructura adecuada (por ejemplo, conectividad, servidores).

Otra condición para la implementación de un piloto de este tipo es el diseño de una interfaz de usuario amigable. De lo contrario, se corre el riesgo de incumplir el objetivo de mayor transparencia y auditoría ciudadana de las transacciones.

Reflexiones finales del caso

Este caso evidencia que bajo ciertas condiciones *blockchain* otorga seguridad y transparencia a la asignación de subsidios y puede ser escalable a otros procesos públicos que requieran notarizar transacciones, como compras o licitaciones públicas. El piloto ha permitido que bajo un correcto uso de la tecnología y el establecimiento de contratos inteligentes no sea posible otorgar más de un subsidio a una misma persona. También ha posibilitado la auditoría ciudadana del proceso burocrático en tiempo real. El informe de evaluación del piloto ha identificado varias lecciones aprendidas del caso que vale la pena resaltar de cara a la implementación de pilotos a nivel local, a saber: (i) la necesidad de una voluntad política para emprender procesos de apertura de información; (ii) la existencia de un proceso estandarizado, con pasos y actores claramente identificables; y (iii) el diseño de un piloto simple, con claros potenciales de ser escalable, en un municipio de tamaño razonable (Cepeda et al., 2017).

2.3.

Facilitar la auditoría de la información

La tecnología *blockchain* (principalmente las *blockchain* públicas no permisionadas) facilita la auditoría de la información al asegurar el registro de todas las transacciones, las cuales generan una cadena de bloques que no se puede borrar o modificar sin dejar una huella. Esta característica además permite auditar procesos confiando en la información de la cadena y sin la necesidad de que terceros brinden la información, lo que quita los incentivos a manipularla con fines particulares.

2.3.1. Licitaciones públicas inteligentes: el caso de México

Un informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre México identificó que para 2015 aproximadamente un 21% del presupuesto asignado a la Administración Pública Federal se destinaba a contrataciones públicas (OCDE, 2018), las cuales se realizan de manera electrónica a través del sistema CompraNet. Un sistema de contratación electrónica puede ayudar a incrementar la transparencia y la eficiencia en la asignación de recursos al reducir las interacciones entre funcionarios encargados de las contrataciones y los oferentes. En este contexto, la OCDE ha hecho un diagnóstico y una serie de recomendaciones a CompraNet para mejorar la publicación de la información relativa a todo el ciclo de contratación, el funcionamiento del sistema, el procesamiento de denuncias y su integridad.

Actualmente, los ciudadanos no pueden participar en la auditoría de los procesos de contratación pública sino que existe la figura de testigo social, que es un representante de la sociedad civil que participa en el proceso y revisa su legalidad y transparencia. En este marco la solución de contratos inteligentes basada en la tecnología *blockchain* tiene como objetivo incrementar la confianza ciudadana en los procesos de contratación pública, permitiendo que aquellos que se hayan registrado puedan participar del monitoreo social de las adquisiciones. También permite a los evaluadores certificados votar y calificar las propuestas de manera anónima, otorgando más transparencia al proceso y eliminando intermediarios para proveer la información sujeta a auditoría.

Descripción de la solución

El piloto de contrataciones inteligentes fue lanzado en 2018 y tiene como objetivo diseñar un sistema de contrataciones basado en *blockchain* y un estándar de contrataciones abiertas que fomente la transparencia de los procesos y su auditoría social. Dentro de las innovaciones previstas para esta solución, se plantea la introducción de la figura de los evaluadores independientes, lo que otorga voz y voto a los ciudadanos para evaluar propuestas, a diferencia de la figura del testigo social. Por otra parte, el estándar de contrataciones abiertas le brinda una mayor integridad a la información del proceso de contratación.

La solución plantea una infraestructura híbrida montada sobre la Red Federal mencionada en la primera parte, la cual utiliza una instancia de Ethereum. Las fases del proceso de contratación incluidas en el piloto son:

I Planificación: se realiza la asignación presupuestaria y se identifican las unidades compradoras y empresas.
II Licitación: se evalúan las propuestas a través de contratos inteligentes, lo cual fomenta la transparencia y evita errores manuales.
III Identificación del ganador: luego de la respectiva evaluación técnica y la posterior apertura de sobres financieros, el sistema asigna al ganador de forma automática.
IV Contratación: se realiza el monitoreo de pagos y cumplimiento de entregables en el sistema.
V Evaluación del proyecto: se genera una reputación a quienes realizan buenas evaluaciones.

De esta manera, se espera que el proyecto piloto de licitaciones inteligentes genere información segura y confiable, garantizando la trazabilidad en tiempo real y fomentando la transparencia en los procesos de contratación.

Tecnologías complementarias

El uso de datos abiertos, en particular el estándar de contrataciones abiertas,[19] puede ayudar a visibilizar los procesos y por tanto las auditorías de contrataciones. Sin embargo, esto no asegura la integridad en el tiempo de la información almacenada en servidores públicos.

Aunque también hay otras medidas organizacionales y/o técnicas que tratan de asegurar la integridad de los datos y, por ende, que tratan de impedir la manipulación ilícita de datos e incorporan reglas para verificar su integridad (por ejemplo, restricciones en el número de personas que pueden manipular la base de datos de los procesos de compras o la publicación en tiempo real de la información de los procesos en formatos

[19] Para entender mejor el estándar, puede visitarse: *https://www.open-contracting.org0/?lang=es*.

abiertos), la tecnología *blockchain* parece tener una ventaja comparativa para dificultar la manipulación o falsificación de los datos en comparación con otras tecnologías si la arquitectura organizacional está bien diseñada.

Consideraciones de implementación

Cabe mencionar que el principal desafío de implementación que enfrenta el escalamiento de la solución es el relacionado con el marco legal. En la actualidad la legislación mexicana contempla únicamente la figura del testigo social, lo que no permite a ciudadanos realizar un monitoreo de las adquisiciones gubernamentales de manera directa como parte del comité evaluador. Tampoco existe regulación vinculada a la información que puede "escribirse" en la cadena de bloques.

Otra consideración para la implementación se vincula al entendimiento del ecosistema en el cual se inserta la solución. Para que la tecnología permita auditar estos procesos de contratación, se necesita una contraparte que la entienda y pueda utilizarla. El piloto ha probado que puede generarse una infraestructura que habilite la transparencia y la estandarización del proceso, pero requiere un análisis más profundo de quienes son los potenciales usuarios de la plataforma y si tienen las capacidades técnicas para poder hacerlo.

Reflexiones del caso

Este caso es particularmente valioso por dos razones. En primer lugar, intenta resolver el problema de falta de transparencia e integridad de la información en los procesos de licitación pública, dado que automatiza aquellos pasos que están expuestos a mayor corrupción –el más relevante de ellos es la evaluación técnica y económica de propuestas– y busca maneras de fomentar la participación ciudadana a través de la evaluación de propuestas y el monitoreo de las contrataciones. Si bien el piloto ha probado que puede generarse una infraestructura para estandarizar y mejorar el proceso de contratación pública, a fin de democratizar el uso de la solución se requiere conocer a los potenciales usuarios de la plataforma y analizar si tienen las capacidades técnicas para poder hacerlo.

En segundo lugar, este piloto sirve como caso de uso para la generación del ecosistema en el marco de la Red Federal impulsada desde la CEDN. Se espera que la evaluación de este aplicativo genere incentivos para el desarrollo de esta Red, el diseño de nuevos casos de uso por parte de los actores de este incipiente ecosistema y el fortalecimiento de su gobernanza.

Recuadro 2

Blockchain para la mejora de los procesos de compras públicas: el caso de Chile Compra

En los últimos años Chile Compra se ha enfocado en mejorar sus procesos y hacerlos más transparentes y confiables, para lo cual ha experimentado con diversas tecnologías que le permitan cumplir con este objetivo. En este contexto ha implementado un piloto basado en el uso de *blockchain* para certificar las órdenes de compra, de manera tal de lograr trazabilidad en el proceso de licitación o compras del gobierno (Jolías, 2018).

El piloto comenzó por las microcompras, que son adquisiciones de montos bajos que pueden realizarse a través de pagos electrónicos y se gestionan a través del portal Mercado Público. Se certificó el contenido de las órdenes de compras de tres organismos del Estado (la Contraloría General de la República, la Dirección de Compras y Contratación Pública y el Servicio de Impuestos Internos) en la red pública Ethereum; los datos de la orden de compra pasan a ser un *hash* que posteriormente se certifica en la red y se incorpora a la cadena de bloques. De esta manera, los proveedores y personas interesadas pueden corroborar que la información no ha sido alterada ni manipulada; para esto, se ha diseñado una interfaz amigable que permite verificar el certificado de confianza vinculado a la orden.

Dado el éxito del piloto, en la actualidad Chile Compra está evaluando escalar el uso de *blockchain* en las ofertas de los procesos de licitación (comenzando por un proceso simplificado) y la automatización de su evaluación.

2.4.
Asegurar la integridad de los datos

Blockchain permite mejorar y proteger la integridad de los datos al hacer muy difícil la posibilidad de manipularlos sin dejar una huella. Por su diseño intrínseco[20] la tecnología impide la posterior manipulación de datos almacenados en los bloques de la cadena sin que lo perciba el resto de los participantes. La consistencia en los datos entre todos los nodos genera seguridad sobre su integridad,[21] lo cual incentiva la eliminación de intermediarios.

Una función importante del gobierno es mantener información confiable sobre individuos, organizaciones, activos y actividades. La gestión de estos registros suele ser complicada principalmente porque la mayoría de esta información se encuentra en papel. Las agencias de gobierno tienden a construir sus propios silos de datos y protocolos de gestión de la información, lo que impide que otras partes del gobierno los utilicen.

Almacenar un registro de la propiedad en una red distribuida mejora en gran medida su seguridad al eliminar el riesgo de un punto único de falla y hacer más difícil su manipulación. Con esto también se puede aumentar la transparencia y mantener la integridad de los registros permitiendo a los agentes certificados (incluidos, potencialmente, auditores u organizaciones sin fines de lucro) monitorear los cambios realizados en el registro casi en tiempo real y mejorar la eficiencia al reducir el tiempo y dinero asociados con el registro de la propiedad (Pisa y Juden, 2017).

2.4.1. Registro de la propiedad de tierras: el caso de Georgia

Desde 2004 la Agencia Nacional de Registro Público (NAPR, por sus siglas en inglés) de la República de Georgia ha realizado varios procesos de restructuración organizacional, numerosos cambios legales y la digitalización de los archivos, los cuales han mejorado su eficiencia y efectividad significativamente (Weiss y Corsi, 2017). Sin embargo, la NAPR estaba buscando formas de modernizar sus servicios al ciudadano, manteniendo la seguridad de los datos

[20] En la tercera parte de esta publicación se presenta un detalle del proceso de minado de los bloques.

[21] Este atributo pierde robustez en la medida en que el número de actores y nodos participantes disminuye.

del registro de la propiedad, pero permitiendo la transferencia de títulos de propiedad de forma electrónica con mínima interacción personal. En este contexto se ha evaluado la viabilidad de utilizar la tecnología *blockchain* para enfrentar estos desafíos.

Descripción de la solución

En abril de 2016, la NAPR de la República de Georgia decidió diseñar una solución basada en *blockchain* para la gestión de sus registros de propiedad. En una primera fase, se utilizó una *blockchain* privada autorizada para mantener registros críticos, y una *blockchain* pública de Bitcoin para permitir a los ciudadanos verificar el registro de transacciones de transferencia de títulos de propiedad (Graglia y Melon, 2017).

Uno de los elementos centrales de la solución es la publicación de *hashes* de documentos de transferencia de títulos de propiedad en la *blockchain* pública de Bitcoin. Al *hashear* un documento y publicar el *hash* en una cadena de bloques pública se pueden conseguir los beneficios de un notariado (es decir, la verificación/garantía/certificación de la integridad del documento) sin la necesidad de un intermediario. Teniendo en cuenta la dificultad de cambiar información de la cadena (especialmente si es pública), una vez que se publican los *hashes*, el documento tiene una marca de tiempo (Graglia y Melon, 2017). Esto permite a los ciudadanos verificar si una transacción de transferencia de títulos de propiedad ha sido registrada (concretamente en la cadena de bloques) de acuerdo con el certificado de registro que ellos han obtenido al final del proceso. También se asegura la integridad de los datos almacenados, previniendo su falsificación y facilitando la auditoría de la información histórica casi en tiempo real.

Sin embargo, debido a que los documentos y las transacciones asociadas que se almacenan se colocan en una base de datos de *back-end* de la NAPR en la primera fase del piloto, los ciudadanos aún necesitan visitar las oficinas de la NAPR para completar las transacciones (Graglia y Melon, 2017). Es por ello que en febrero de 2017 la NAPR consideró que el programa era viable y que podía aplicarse más ampliamente la tecnología *blockchain* a las transacciones de propiedades, introduciendo contratos inteligentes para simplificar y automatizar las operaciones comerciales, incluida la venta de propiedades y la transferencia, entre otras (Exonum, n.d.).

Actualmente, cuando la NAPR recibe la aplicación para registrar un cambio de propiedad en el proceso tradicional, comprueba que la propiedad le pertenece al vendedor y que no hay gravámenes impagos en ella antes de transferir la propiedad. Mientras la NAPR está realizando el proceso, tanto el vendedor como el comprador pueden cambiar de opinión (antes o después de efectuarse el pago), con lo que pueden generarse conflictos que luego podrían llevar mucho tiempo de resolución en la justicia. Los ciudada-

nos usualmente protegen sus intereses contratando a notarios y bancos como intermediarios; sin embargo, esto es costoso (Weiss y Corsi, 2017).

Al introducir contratos inteligentes a la solución, los ciudadanos que quieran vender una propiedad pueden iniciar una sesión en el sitio web de la NAPR, acceder a los datos relativos a su propiedad y ponerla a la venta. Los interesados pueden realizar ofertas y si alguna resulta atractiva, los vendedores pueden aceptarla. La disponibilidad de fondos por parte del comprador y la confirmación de la propiedad por parte del vendedor pueden hacerse automáticamente, y entonces la transacción se cierra. La información de compra estará disponible en la cadena de bloques pública. Cabe destacar que el piloto se diseñó de forma tal que si la cadena de bloques no funcionaba correctamente, se volvería al esquema anterior automáticamente (Weiss y Corsi, 2017).

Si todas las transacciones vinculadas a la transferencia de títulos de propiedad están registradas en la cadena de bloques (el registro de propiedad y las transacciones financieras que corresponden a su transferencia), y todas las partes involucradas (vendedor, comprador, bancos, gobierno) confían en la integridad de los datos, una transferencia de propiedad podría realizarse electrónicamente, sin intermediarios y en tiempo casi real (dependiendo del mecanismo de consenso usado).

Mediante el uso de contratos inteligentes, en el futuro la agencia podría beneficiarse del potencial de automatizar pasos del proceso de registración de títulos de propiedad que hasta ahora han necesitado la intervención manual de funcionarios del gobierno.

Consideraciones de diseño para aprovechar el potencial de la tecnología

Como se observa en este caso, *blockchain* puede ayudar a resolver problemas relacionados con la confiabilidad e integridad de los registros públicos. Sin embargo, la tecnología es un sistema basura dentro, basura fuera; es decir, si la información que se carga en el sistema es falsa (ya sea por descuido o engaño), la información escrita en la cadena será falsa también (Pisa y Juden, 2017).

También es importante definir roles y permisos de los distintos actores que utilizarán y/o editarán estos registros en el caso de la *blockchain* privada. Para garantizar la consistencia de los datos entre los nodos, es importante definir cómo, cuántos y bajo qué autoridad estarán distribuidos los nodos de la red. Si existe solo un nodo, los datos no son más seguros que en bases de datos tradicionales no replicadas (incluso se podría cuestionar si el término *blockchain* es aplicable en este caso). Además, la replicación de los datos a múltiples nodos podría impedir la pérdida de información si uno (o un número insignificante) de los nodos falla.

Recuadro 3

Time stamping para proteger la integridad de las leyes argentinas

La República Argentina publica las leyes del Congreso y actos del Poder Ejecutivo a través del Boletín Oficial, que cuenta con una versión en línea *(https://www.boletin-oficial.gob.ar/)* donde se difunde el contenido en formato PDF. La publicación en el Boletín es obligatoria para la entrada en vigor de una normativa.

La Secretaría Legal y Técnica de Presidencia de la Nación, junto con la Secretaría de Modernización de Jefatura de Gabinete de Ministros, ha diseñado un proceso de certificación basado en *blockchain* para generar un recibo digital con la fecha y hora de una transacción *(time stamping*), que permite comprobar si la versión en PDF del Boletín corresponde a la edición publicada en *blockchain*. Cuando se publica la edición diaria en formato electrónico del Boletín, se genera un *hash* con su contenido. Este se utiliza para generar una transacción en el BFA a través de una operación de *time stamping*. De esta manera, se obtiene una prueba que permite afirmar la existencia de una edición específica del Boletín, inalterable respecto de la edición original.

Además de ser una solución que brinda integridad y transparencia al proceso de publicación de las normativas, este caso es uno de los primeros en formar parte de la plataforma pública abierta BFA, cuyo objetivo es integrar servicios y aplicaciones basados en la tecnología *blockchain* generados por el ecosistema digital argentino.

Otras tecnologías

Finalmente, es necesario mencionar que la gestión de registros públicos y el intercambio de datos entre diferentes autoridades (incluyendo instituciones financieras) también puede realizarse con otras tecnologías como, por ejemplo, las bases de datos comunes o la sincronización de bases de datos separadas mediante API. Sin embargo, estas alternativas no tienen el nivel de seguridad ni brindan la posibilidad de integrarse con sistemas diferentes como otorga *blockchain*. Mientras que en el caso de las bases de datos la seguridad de que los archivos no hayan sido manipulados recae en los permisos que se den a nivel de usuario (normalmente solo los administradores de la base de datos pueden hacerlo), en *blockchain* la seguridad viene dada por la criptografía de las funciones *hash*. Por su parte, conectar bases de datos de instituciones diferentes mediante API en muchos casos es sencillamente inviable ya que puede significar integrarlos fuertemente lo cual podría no ser deseable.

Reflexiones finales del caso

El principal valor añadido por el uso de *blockchain* en este caso es un aumento en la seguridad y confiabilidad de los certificados (Allessie et al., 2019). La solución tecnológica ha permitido una mayor transparencia en el proceso de registro de los títulos de propiedad, aunque los ciudadanos solamente tienen medios limitados para verificar los datos debido al uso de una *blockchain* privada autorizada para el manejo de la información relacionada a la registración de títulos de propiedad, lo cual los excluye del proceso de auditoría.

Por último, el piloto trae mejoras significativas en términos de eficiencia y efectividad de la registración y verificación de los títulos de propiedad: el tiempo de entrega del servicio de registración se ha reducido de entre uno y tres días hábiles a varios minutos; el tiempo de verificación de certificados se ha reducido de unos pocos días a unos segundos; los costos operativos del servicio de registro se han reducido en un 90% (Weiss y Corsi, 2017; Allessie et al., 2019).

2.5.

Tokenizar activos y registros públicos

Tal como se mencionó anteriormente, una solución basada en *blockchain* puede permitir expresar algunos activos como *tokens,*[22] de manera de contar con un registro confiable de los cambios y reducir la cantidad de intermediarios e interacciones que intervienen en las transacciones que lo vinculen. Por ejemplo, puede utilizarse para administrar una cadena de suministros (como de medicamentos o alimentos), rastrear activos, dar valor a la propiedad de un bien (como una obra de arte), seguir inventarios o cualquier otra transacción que requiera documentar eventos vinculados a un activo. De esta manera, se incrementa la confianza en el activo al permitir su trazabilidad (Berryhill, Bourgery y Hanson, 2018). Otra aplicación, más vinculada al sector privado, es la de compensar a participantes de una red (a través de la creación de dinero virtual) y/o brindar derechos de participación en la propiedad de un activo a cambio de recibir compensaciones ante aumentos futuros en su valor (McKinsey, 2018). De acuerdo con Wachal (2018),[23] la tokenización de activos permite convertir los derechos de un activo con valor económico en un *token* digital, los cuales luego serán alojados y gestionados en una red de *blockchain*.

2.5.1 El mercado del arte y la tokenización de activos

En la actualidad, no existen en la región casos de tokenización de activos en el sector público. Sin embargo, su potencial de uso es alto para generar activos digitales; por ejemplo, dentro del proyecto de *blockchain* vinculado al Barrio 31 que se verá más adelante, se prevé analizar la viabilidad de tokenizar certificados de propiedad, vivienda, trabajo y méritos académicos.

Un caso que resulta atractivo a la hora de ejemplificar el valor de tokenizar activos proviene del mercado del arte. En este mercado intervienen un gran número de intermediarios (galerías, coleccionistas, subastas, etc.) y a la hora de adquirir una pieza se requiere comprar el activo completo. El proyecto Maece-

[22] Cabe destacar que existen diferencias regulatorias entre los *tokens* de valor que se revisan en este apartado y las criptomonedas. Para un mayor detalle, véase: https://sites.duke.edu/thefinregblog/2018/11/16/tokenomics-crypto-asset-valuation-token-design-and-the-development-of-blockchain-networks/.

[23] Más información disponible en: https://blog.softwaremill.com/asset-tokenization-on-blockchain-will-disrupt-the-asset-management-landscape-befbd71639b1.

nas[24] tiene como objetivo generar una plataforma para comerciar las obras de arte de manera descentralizada y disponible para las personas. A través de la tokenización de una obra (dividiéndola en unidades financieras digitales) (Maecenas, 2018), una persona interesada puede convertirse en propietario de una parte de ella e intercambiarla cuando lo requiera. El monto mínimo para participar se reduce, así como la cantidad de intermediarios en la transacción y las asimetrías de información en cuanto al valor de la obra.

Condiciones para implementar esta solución con tecnología blockchain

Tal como sucede con las criptomonedas, se necesita de una regulación robusta que habilite el uso de los *tokens* para transacciones, definiendo su valor como representación digital de un activo físico y considerando la diversidad de aplicaciones que puede tener.

Es importante notar que este tipo de aplicaciones en donde se debe vincular un activo físico a un activo digital requiere confiar en una entidad u organización que se encargue de establecer esa vinculación. Este rol, al que se denomina oráculo, en sentido estricto se enfrenta a uno de los principales objetivos iniciales de la tecnología (eliminar la necesidad de confiar en alguien). Debido a los otros beneficios identificados (división de la propiedad, eliminación de intermediarios, mercados eficientes), y en la medida en que aún se cuenta con un alto grado de eliminación de necesidad de confianza entre los actores, se considera que la tokenización de activos será uno de los más prometedores casos de uso de la tecnología.

Tecnologías alternativas

En sentido estricto, si se tiene que confiar en el oráculo para la vinculación entre el activo físico y el virtual se podría utilizar una base de datos centralizada que el mismo oráculo administre para realizar y registrar las transacciones. Las ventajas de *blockchain* residen en la distribución de información y la reducción del riesgo con el oráculo en la vinculación del activo virtual con el físico, pero no en las transacciones entre participantes.

Reflexiones del caso

Este caso permite demostrar que *blockchain* habilita la representación de un activo físico de manera digital. De esta forma, la propiedad de un activo puede ser divida e intercambiada en el mercado sin la necesidad de intermediarios.

[24] Para conocer más del proyecto visítese: *https://www.maecenas.co/*.

2.6.
Facilitar la automatización de los procesos públicos

Si bien la automatización de procesos ha sido implementada en el sector público previamente al surgimiento de *blockchain*, la distribución de los registros, junto con el establecimiento de los contratos inteligentes que permite la tecnología, puede facilitar este proceso. Por ejemplo, en aquellos casos en que los pasos de los procesos públicos dependen de cambios en el estado de otros procesos (en *blockchain* se reflejan en los datos almacenados en los bloques de cadena) los contratos inteligentes podrían desencadenar los pasos subsiguientes de forma automática sobre la base de reglas predeterminadas y sin la necesidad de intermediarios, de manera de evitar cambios unilaterales.

2.6.1. Automatización de procesos de contratación pública en los Estados Unidos

La GSA es una agencia independiente del gobierno de los Estados Unidos, creada en 1949 para apoyar el funcionamiento básico de las agencias federales (GSA, 2017). La GSA establece contratos gubernamentales a largo plazo con compañías comerciales para proporcionar acceso a millones de productos y servicios a un precio de descuento por volumen.[25]

El sistema actual de contratación pública de la GSA data de los años ochenta. Aunque el sistema está completamente digitalizado, sus procesos son complejos e implican varios pasos manuales. Las propuestas de licitadores están guardadas en el sistema como datos no estructurados en formato PDF. El problema principal del sistema actual es que el proceso de contratación pública es muy lento: desde la presentación del tiempo hasta la conclusión del contrato se toma en promedio 110 días.

Con el objetivo de optimizar los procesos de adquisición pública, la GSA analizó el proceso comercial de los contratos Schedule 70 e identificó los dos procesos más largos en la ruta crítica: (i) el

[25] Los GSA Schedule Contracts, también conocidos como GSA Schedules o Federal Supply Schedules son entregas indefinidas en cantidades indefinidas (*indefinite delivery, indefinite quantity* [IDIQ]), con contratos a largo plazo bajo el programa Multiple Award Schedule de la GSA.

análisis financiero de la compañía y (ii) el memorando de prenegociación. En la revisión financiera el proceso tradicional involucraba a un empleado que extraía información financiera del material proporcionado por el proveedor y calculaba el estado financiero de la empresa, lo que llevaba hasta un mes. En cuanto al memorando de prenegociación,[26] el proceso tradicional involucraba múltiples correos electrónicos entre el gobierno y el proveedor, y sucesivos intercambios con el oficial contratante para revisar múltiples sistemas (Thornton, 2017).

Descripción de la solución

Para modernizar su sistema, la GSA está considerando utilizar una combinación de diferentes tecnologías, como *blockchain* e IA. El objetivo es generarle valor al contribuyente, disminuir la carga en la industria y liberar a los profesionales de las tareas orientadas a procesos para que puedan dedicar más tiempo a enfocarse en el pensamiento crítico (Thornton, 2017). Con respecto al tiempo de entrega, la GSA espera realizar procesos de contratación en menos de 10 días después de la optimización de sus procesos de adquisición (Friedman, 2017).

En una primera fase la GSA realizó una prueba de concepto para optimizar los procesos comerciales de los contratos Schedule 70 en el año fiscal 2017. La prueba de concepto involucró la utilización de varias tecnologías para aumentar la eficiencia de los procesos implicados. Como base de la nueva solución, la tecnología *blockchain* proporciona una capa de datos con todas las transacciones y a la que todos los interesados pueden acceder en tiempo real (Thornton, 2017). La GSA controla lo que los participantes en el mercado pueden ver de acuerdo con ciertas reglas asociadas de la industria (por ejemplo, no compartir la información de múltiples socios de la industria entre sí).

Como se menciona a lo largo de esta publicación, la tecnología basada en *blockchain* públicas se vuelve menos eficiente cuando hay más información en la cadena. Para solucionar esto, la GSA separó archivos grandes asociados con las entradas, fotos y videos, y los colocó en una base de datos separada e inmutable. En la cadena de bloques solo conservan la información necesaria para la automatización de modo que la cadena pueda funcionar de manera flexible y rápida (Goldstein, 2018).

Adicionalmente, la nueva solución usa contratos inteligentes para automatizar pasos seleccionados del proceso que antes eran manuales. Según la GSA, podrían haber automatizado sin usar *blockchain* pero esta tecnología proporciona un registro de todas las interacciones a las que ambas partes pueden acceder en tiempo real, lo cual permite

[26] Se trata de un documento preparado para las negociaciones de la GSA con un proveedor donde figuran los temas a plantear en la negociación.

que los microservicios sean más precisos sin tener que tomarse el tiempo para conciliar dos versiones separadas del mismo documento (Thornton, 2017). Por último, un flujo de trabajo optimizado y una interfaz de usuario rediseñada facilitan que la industria solo tenga que ingresar la información una vez en lugar de iniciar sesión en múltiples sistemas (Thornton, 2017; Goldstein, 2018). En una segunda fase la GSA planea implementar y desplegar un piloto en los años fiscales 2018/19 para finalmente escalar la nueva solución a todos los procesos del programa Multiple Award Schedule en los años financieros 2019 a 2021.

Tal como se ha mencionado, en la revisión financiera el proceso tradicional involucraba a un empleado que extraía información del material proporcionado, lo que llevaba hasta un mes. Luego de la prueba piloto el proceso es casi instantáneo y la revisión se hace de manera automatizada, prescindiendo de terceros. Las ofertas que pasan van al siguiente eslabón en el flujo de trabajo; aquellos señalados para su posterior revisión o rechazados se envían a un revisor humano para su análisis. Asimismo, a través del historial completo de entradas, *blockchain* se convirtió en el sistema de registro de una oferta completa, que permitió reemplazar múltiples correos electrónicos entre el gobierno y el proveedor para preparar la carta de prenegociación, y evitar idas y venidas con el oficial contratante para revisar múltiples sistemas. Como consecuencia, se ha reducido el tiempo para preparar la carta de entre 15 y 30 días a menos de 10 días (Kelman, 2017).

Condiciones para implementar esta solución con tecnología *blockchain*

Cabe aclarar que la tecnología solo asegura la auditabilidad de aquellos datos que son parte de la cadena de bloques. En el caso de ingresar datos incorrectos o falsificados en la cadena de bloques, esta tecnología considera que representan la "verdad" al momento de la entrada y así forman el historial sujeto a auditoría. Por ello, es importante que en el diseño de la solución tecnológica se incluya un rediseño de los procesos organizacionales, generando protocolos adecuados que impidan la entrada de datos falsificados desde el principio. También se necesita contar con la información digitalizada y una clara definición de los elementos que van a formar parte de la cadena, de manera tal de optimizar el tiempo de procesamiento de las transacciones poniendo información crítica del proceso.

Tecnologías alternativas

Al igual que en el caso anterior, la tecnología *blockchain* no es la única que facilita la auditoría de los procesos públicos. Otras herramientas, como los archivos de registro (*log files*), también pueden hacer comprensible el historial de modificaciones de los datos en otras tecnologías como son las bases de datos. La ventaja de la tecnología *blockchain* es que la historia no puede ser manipulada por alguno de los nodos sin ser visto por el resto de los partici-

pantes; mientras que en el caso de los archivos de registro una manipulación sería posible si no se han introducido medidas adicionales para protegerlos de accesos ilícitos.

Reflexiones del caso

El principal valor añadido por el uso de *blockchain* en este caso es el manejo de un conjunto de datos y transacciones de forma segura y confiable, lo cual facilita la automatización de los procesos. Para el caso particular de las compras públicas, donde la confianza en la integridad de los datos es clave y generalmente demanda tiempo y recursos, una solución basada en *blockchain* y otras tecnologías disruptivas brinda una mayor eficiencia al proceso.

La prueba de concepto identificó varias ventajas del nuevo proceso: (i) brinda mayor rendimiento; (ii) reduce el tiempo del ciclo (menos de 45 días); (iii) simplifica el proceso de oferta; (iv) conecta sistemas de la tecnología de la información y la comunicación (TIC) heredados dispares; (v) permite a las partes confiables intercambiar datos críticos rápidamente sin necesidad de costosas infraestructuras de intercambio electrónico de datos y de mensajería; y (vi) acelera el uso de la tecnología emergente en el ámbito federal.

Desde una perspectiva de costos, la GSA cree que la implementación de la nueva solución reducirá los costos directos de analizar una propuesta en casi un 80%. Su objetivo es reducir el tiempo de incorporación de los contratos programados de 110 días (proceso normal), y de 40 días (proceso simplificado) a menos de 10 días con la nueva solución (Thornton, 2017).

2.7.

Generar credenciales digitales

En la economía digital las credenciales digitales son necesarias para demostrar de manera electrónica alguna acreditación que las personas tienen (desde certificados de vacunación hasta títulos profesionales o experiencia laboral). Aplicado al mercado laboral, estas credenciales describen académica y laboralmente a los candidatos, y les sirven a los empleadores para verificar si la experiencia se vincula a las demandas de un puesto de trabajo, además de asegurarles que estos certificados fueron emitidos por las instituciones que las personas indican.

En la actualidad las personas dependen de certificados físicos altamente vulnerables (falsificables) para demostrar sus credenciales. Adicionalmente, la generación de estos documentos físicos toma muchas veces años, pues los procedimientos son extremadamente lentos. Universidades y empresas ofrecen servicios de verificación de credenciales, pero muchos empleadores no los utilizan o son muy ineficientes y costosos. Por su parte, una consulta electrónica requeriría de una adecuación de sistemas y la adopción de estándares mínimos por parte de todos los involucrados.

La tecnología *blockchain* puede ayudar a certificar y verificar estas características de manera segura y a su vez puede poner en manos de la persona el control sobre sus registros laborales y académicos.[27] Tal como se mencionó anteriormente, el uso de *blockchain* para certificar información puede permitir que sean las personas las que "porten" su información personal digitalizada, aprobando y permitiendo su acceso con mayor control.

2.7.1. Certificados digitales para fortalecer el mercado laboral: el caso de Bahamas

En la actualidad se está analizando el potencial de la tecnología *blockchain* para generar un mercado laboral más transparente[28] y adecuado a las necesidades del mercado a nivel global. A través de los *blockcerts, un* estándar abierto para credenciales digitales creado por el laboratorio del Instituto Tecnológico de Massachusetts (MIT Media Lab, por sus siglas en inglés) en 2016,[29] pueden emitir y eventualmente verificar certificados de formación laboral de una persona. De esta manera, un trabajador que se ha formado en línea y ha obtenido certificados de diversas instituciones a nivel global puede portar los registros de sus habilidades y experiencia de manera segura y digital.

El gobierno de Malta fue el primero en experimentar con blockcerts en el sector educativo. En la región el gobierno de Bahamas emitió en 2018 los primeros 78 certificados digitales a través de la Agencia Nacional de Capacitación (NTA, por sus siglas en inglés) en *blockchain*. Bahamas Blockcert ha implementado un piloto con los certificados de capacitación de esta entidad, pero está explorando la manera de incluir nuevos sectores para verificar otros

[27] Para más información, visítese: *https://er.educause.edu/articles/2017/4/credentials-reputation-and-the-blockchain*.

[28] Puede leerse al respecto en: *https://blogs.iadb.org/trabajo/es/blockchain-como-la-tecnologia-puede-mejorar-el-mercado-laboral/*.

[29] Para conocer más, visítese: *https://er.educause.edu/articles/2017/4/credentials-reputation-and-the-blockchain*.

certificados (tributarios, licencias comerciales, etcétera.).[30]

Descripción de la solución

El proyecto Bahamas Blockcert permite la emisión de certificados digitales validados a nivel nacional con un formato abierto e interoperable, por lo que pueden alojarse en diversas plataformas. En este caso se utiliza una billetera digital, a la que se accede a través de una aplicación móvil. Además de poder alojar y portar sus *blockcerts*, las personas tendrán la posibilidad de agregar su currículum vítae y otros atributos de identidad (ID, tarjeta de seguro social, licencia de conducir). Adicionalmente, podrán enviar estas certificaciones a potenciales empleadores, los cuales pueden verificar la autenticidad de la información. Como consecuencia, se intenta remover barreras al acceso de información y hacer más eficiente la búsqueda laboral.

La tecnología *blockchain* brinda seguridad y certeza a los *blockcerts*, pero además elimina intermediarios que anteriormente debían certificar la validez de los títulos académicos, cursos de capacitación y certificaciones. Debido a que la verificación de esta información se puede automatizar, pueden ahorrarse tiempos y costos de transacción vinculados al reclutamiento.

Dado el éxito del piloto, en la actualidad se está evaluando la posibilidad de emitir *blockcerts* para obtener licencias de negocio, las cuales requieren de la verificación de varios documentos. Como primer paso, se espera poder emitir estos certificados como *blockcerts* para luego emitir certificados digitales de todos los documentos requeridos para el trámite, automatizando el proceso.

Por último, la Universidad Provincial del Sudoeste de la Provincia de Buenos Aires (UPSO) de Argentina ha implementado un piloto de certificación de títulos académicos emitidos por esta universidad a través de la emisión de *blockcerts*.[31] También se está utilizando este protocolo para emitir certificados a fin de habilitar el consumo de alcohol en locales del Municipio de San Nicolás de los Garza en el estado de Nuevo León, México.

Condiciones necesarias de implementación

Tal como se menciona en la primera parte, el éxito en la implementación y escalamiento de un proyecto de estas características depende en gran medida de la generación de un ecosistema digital que emita y utilice estos certificados. Pero también requiere la generación de habilidades digitales tanto para los usuarios como para quienes deben gestionar esta información.

30 Más información disponible en: *https://blogs.iadb.org/caribbean-dev-trends/en/the-bahamas-pioneers-blockcerts-for-development/*.

31 Puede leerse al respecto en: *https://www.lanueva.com/nota/2019-1-5-12-37-0-el-blockchain-se-acerca-a-bahia-la-upso-se-convirtio-en-la-primera-universidad-en-dar-certificados-imposible-de-falsear*.

Tecnologías alternativas

Una manera de acreditación digital puede ser la publicación de una base de datos oficial con todas las certificaciones existentes para consulta pública. Alternativamente, podría crearse un servicio de búsqueda de certificaciones, la cual podría accederse al introducir información básica de un ciudadano, como su número de cédula de identidad. Finalmente, también podría incluirse un API para facilitar la integración de este servicio de búsqueda.

Si bien esto podría funcionar para cierto tipo de información (por ejemplo, la que publica la Superintendencia Nacional de Educación Superior Universitaria de Perú sobre titulación) existen otros tipos de certificaciones que por razones legales (protección de datos personales) o prácticas (certificados detallados de notas) complicarían este mecanismo. En general, esta opción no garantiza contar con la autorización del ciudadano para compartir la información.

Otra alternativa podría consistir en una solución parecida a los *blockcerts*, pero sin la necesidad de utilizar una implementación sobre *blockchain*. Es decir, regresando al caso de la Superintendencia Nacional de Educación, el ministerio de educación podría darle a cada ciudadano la capacidad de acceder a su información a través de la generación de un código de respuesta rápida (QR, por sus siglas en inglés) cada vez que este desee mostrar su credencial, la cual podría luego ser validada por el empleador en la página web del ministerio o a través de una aplicación. Si bien esto podría ser una buena solución al problema, los requerimientos para que esta información pueda ser utilizada entre distintas entidades y/o sectores o incluso entre distintos países podrían generar costos adicionales.

Reflexiones del caso

El principal valor añadido por el uso de *blockchain* en este caso es un aumento en la seguridad y certeza de los certificados digitales. Además, la tecnología facilita la eliminación de intermediarios que anteriormente debían certificar la validez de los títulos académicos, cursos de capacitación y certificaciones, da a los ciudadanos mayor control sobre sus credenciales (autosoberanía, protección de privacidad) y habilita la automatización de la verificación de esta información a través de un estándar abierto, ahorrando tiempos y costos de transacción vinculados al trámite de validación y a los procesos que dependen de estos certificados (por ejemplo, reclutamiento de personal).

2.8.

Construir una identidad digital y soberana

A diferencia de la identificación digital, que se enfoca en la posibilidad de identificar a una persona por medios electrónicos, la identidad digital hace referencia a una colección de atributos capturados y almacenados electrónicamente que describen de manera única a una persona dentro de un contexto dado.

La identidad digital de una persona, por lo tanto, puede estar compuesta por una variedad de atributos, incluidos datos biográficos (por ejemplo, nombre, edad, sexo y dirección) y datos biométricos (por ejemplo, huellas dactilares y escaneos de iris), así como otros más amplios relacionados con las actividades que la persona realiza en línea o algo que otra persona, empresa o institución sabe sobre aquella (por ejemplo, visitas médicas, escolaridad, compras, etc.).

Debido a que el mundo digital actualmente no tiene una capa de identificación nativa[32] que permita a la persona probar que es quien dice ser en un entorno digital, las empresas y las instituciones públicas han implementado sistemas ad hoc para identificar individuos, lo que ha resultado en la generación de tantas identificaciones como servicios, y donde cada entidad administra una base de datos con sus correspondientes datos de comportamiento y actividades para cada persona. En extremo, cada persona termina teniendo tantas identificaciones digitales como servicios digitales a los que intenta acceder, no siempre vinculados y con atributos digitales alojados con el potencial de ser compartidos para una mayor eficiencia. Desafortunadamente, estas bases de datos son silos de datos incompatibles que producen muchos problemas: poca seguridad y control de los datos por parte de las personas, posibilidad de fraude de identidad, datos alojados por distintas instituciones que pueden ser incompatibles, entre otros (Voshmgir, 2017).

[32] Internet se construyó sin una forma estándar y explícita de identificar personas u organizaciones. El sistema de direccionamiento de Internet se basa en la identificación de puntos finales físicos (máquinas) en una red. Las personas no son puntos finales en una red. Por lo tanto, Internet no tiene forma de identificar personas de manera única. En el pasado esto ha creado considerables costos operativos, de oportunidad y de uso para la economía digital, tanto para las empresas como para los usuarios.

En la actualidad se están diseñando soluciones basadas en la tecnología *blockchain* para desarrollar *modelos de identidad digital soberana*.[33] En el modelo de identidad soberana las personas y las organizaciones pueden almacenar sus propios datos de identidad y proporcionarlos de manera eficiente a quienes necesitan validarlos sin depender de un repositorio central de datos de identidad. Un proceso de identificación según el modelo soberano podría involucrar los siguientes elementos[34] (Lewis, 2017):

I A través de un proceso de registro (*onboarding*) que puede variar según las especificaciones de diseño de la solución, se otorga un número de identificación autogenerado y único para cada persona (llamado identificador descentralizado [DID, por sus siglas en inglés]),[35] con una clave pública y una clave privada asociada. Este proceso de *onboarding* puede involucrar la vinculación del DID con la identidad legal de la persona, de manera de vincular la identificación legal con esta identidad digital descentralizada.

II Junto con este número de identificación (que podría convertirse en un sistema de identificación digital único), el usuario puede crear certificados (afirmaciones de identidad) autenticados por las autoridades relevantes (por ejemplo, certificar su nivel de escolaridad a través de la autenticación otorgada por el Ministerio de Educación). Este DID, en conjunto con los certificados, va a conformar la identidad de la persona.

[33] En general hay dos enfoques para administrar la identidad digital. El modelo centralizado y el modelo descentralizado (Allen, 2016; GSMA, World Bank Group y Security Identity Alliance, 2016; Preukschat, 2018; WEF, 2016). La identidad autosoberana (*self-sovereign identity* [SSI]) es un derivado (*spin-off*) del modelo descentralizado y crea así un tercer enfoque (Preukschat, 2018). En los sistemas de identidad centralizados una sola entidad actúa como un proveedor de identidad que autentica a los usuarios y transfiere sus atributos. En sistemas de identidad distribuidos muchos proveedores de identidades recopilan, almacenan y transfieren atributos del usuario. Estos sistemas no dependen de los atributos de un solo proveedor de identidad, sino que les permite a los usuarios interactuar fácilmente con muchas entidades diferentes en un entorno en línea dándoles una billetera digital de credenciales (WEF, 2016).

[34] En general un sistema de identidad tiene tres componentes básicos: (i) las afirmaciones: son datos provistos por la persona o empresa, (ii) las pruebas: alguna forma de documento que proporciona evidencia para el reclamo y (iii) las certificaciones: la validación por parte de terceros de que, según sus registros, las afirmaciones son verdaderas. Además, hay tres partes involucradas en el proceso de la identificación: (i) los usuarios, (ii) los proveedores de identidad y (iii) la parte que otorga confianza a dicha identidad.

[35] Para un mayor detalle de esta especificación consúltese: https://w3c-ccg.github.io/did-spec/#terminology.

III Estos certificados pueden ser almacenados en una especie de billetera de identidad, una aplicación en un teléfono inteligente o una computadora para poder guardar y gestionar los atributos de identidad a través de afirmaciones (por ejemplo, si la persona es mayor de edad se almacena un sí en lugar de su edad).

IV Finalmente, el usuario puede utilizar estos certificados como información veraz de la identidad. Los certificados pueden almacenarse en el dispositivo de la persona y luego, cuando se solicite, la persona presentará y/o aprobará que un tercero acceda a datos específicos a través de una notificación en su dispositivo.

En una solución de identidad digital soberana basada en la tecnología *blockchain*, los atributos validados y almacenados de manera descentralizada podrían accederse y confirmarse desde una cadena de bloques, lo cual permitiría a cualquier persona buscarlos y recuperarlos con una clave pública asociada. Los proveedores/certificadores de atributos podrían usar claves vinculadas a su atributo para firmar la solicitud, de modo que cualquiera que lo obtenga pueda validar que fue emitido por este. Por otra parte, los usuarios cuentan con diferentes métodos para mostrar distintos atributos validados, incluyendo la posibilidad de hacer pruebas de conocimiento nulo (*zero-kownledge-proofs* [ZNP]), consistentes en demostrar que una información sobre uno mismo es cierta (por ejemplo, que uno es mayor de edad) sin necesidad de ofrecer la información en sí (la edad). En sentido estricto cualquier organización o persona podría certificar cualquier afirmación que desee; los usuarios serán libres de almacenarlas en su identidad; y los solicitantes de credenciales podrían elegir en cuáles confían. Tal como se menciona en el siguiente caso de estudio, el éxito de este modelo depende en gran parte de la generación de un ecosistema que genere y utilice estos certificados y del diseño de una interfaz que permita a las personas alojar certificados y tener efectivo control de su identidad.

2.8.1. Identidad soberana en Argentina: el caso del Barrio 31 en la Ciudad de Buenos Aires

El registro y la gestión de la identidad son instrumentos esenciales para la inclusión, ya que permiten mejorar la calidad de los servicios provistos por el sector público y privado. La identidad digital ayuda a las personas a participar en la economía de muchas maneras: abriendo cuentas, recibiendo dinero, afirmando sus derechos sobre activos digitales, etc., pero establecer esa identidad puede ser un gran desafío, especialmente en países sin esquemas de identidad nacional digitalizada (Mas y Porteous, 2015). En este sentido, el gobierno de Argentina ha realizado numerosos esfuerzos por fortalecer y digitalizar su sistema de identidad; el más reciente de ellos es la creación del Sistema de Identidad Digital,[36] para validar remotamente la identidad de los ciudadanos a través de la autenticación biométrica.

De acuerdo con las cifras más recientes de la Dirección General de Estadística y Censos del Gobierno de la Ciudad de Buenos Aires (GCBA), en la Ciudad Autónoma de Buenos Aires (CABA) viven alrededor de 3.059.000 personas, donde las tasas de pobreza e indigencia son del 16,2% y 3,7%, respectivamente. El Barrio 31 es el asentamiento informal más antiguo y grande de la CABA, donde habitan alrededor de 43.000 personas[37] (aproximadamente el 50% de ellas son menores de 25 años) en un área de 32 hectáreas. La alta densidad de población de este barrio ha generado problemas importantes de hacinamiento y ha agudizado problemas socioambientales. El gobierno de la CABA estima que el 67% de los hogares del barrio se encuentran por debajo de la línea de pobreza. Asimismo, el 22% de los hogares registran condiciones de hacinamiento, comparado con el 1,8% en el resto de la CABA. El 25% de los niños de tres a cinco años no asisten a la escuela y el 64% de los jóvenes de entre 18 y 25 años no han completado

[36] Más información disponible en: https://www.argentina.gob.ar/sid-sistema-de-identidad-digital.

[37] Según el Censo Nacional de Población y Vivienda, en el año 2010 163.000 personas vivían en barrios vulnerables (villas de emergencia) en la CABA. Si se contrastan estos datos con los resultados del estudio realizado por la Secretaría de Hábitat e Inclusión del GCBA en 2014, que indican que 275.000 personas habitan en este tipo de barrios vulnerables, se observa que en cuatro años esta población sufrió un aumento del 68,7%. Asimismo, en 2016 el gobierno de Argentina junto con diferentes organizaciones realizó un estudio en el que se relevaron 4.100 barrios vulnerables en el país, en los cuales viven un estimado de 1.340.272 personas, de las cuales un 38% son niños o jóvenes de hasta 20 años (BID, 2018).

su educación secundaria (BID, 2018). Por otra parte, la penetración de celulares en el barrio ronda el 86%, de los cuales el 76% son *smartphones*.

Entre otras razones, los altos niveles de pobreza y vulnerabilidad existentes en la población que vive en asentamientos informales están relacionados con el concepto de penalización de la pobreza. La literatura presenta varias causas detrás de esta penalización, incluidas las fallas de mercado (por ejemplo, costes logísticos), pero destaca la información imperfecta como un elemento central de dicha penalización. En múltiples situaciones el mercado al no contar con información sobre la identidad y comportamiento de las personas más vulnerables no puede incluirlas o lo hace a un costo mucho más alto que para el promedio de la población (BID, 2018).

El déficit de información vinculado con la penalización de la pobreza incluye en uno de sus planos la falta de información financiera: las personas que habitan en las villas no suelen contar con documentación actualizada y confiable sobre su nivel de ingresos o su historial de transacciones financieras, por lo que no pueden ser evaluadas por el sector financiero tradicional, y de esta forma no acceden a servicios financieros o lo hacen en el sector informal, pagando por ello tasas de interés muy elevadas[38] o costos transaccionales altos (por ejemplo, para el envío de remesas). Esto a su vez dificulta sus actividades productivas, lo cual limita sus oportunidades de generación de mejores ingresos.

Adicionalmente, la información patrimonial de las personas que habitan en asentamientos informales es escasa: los habitantes de estos barrios no tienen un título de propiedad formal,[39] por lo que no pueden utilizar su vivienda (y muchas veces tampoco otros activos físicos) como garantías para el acceso a servicios financieros. Esto a su vez dificulta el acceso a bienes y servicios públicos y privados vinculados con la existencia de una dirección física. La escasez de información también afecta el plano formativo y ocupacional: los habitantes de los barrios por lo general cuentan con un limitado registro formativo (títulos académicos, certificados de formación, etc.) y de experiencia laboral formal, situación que les dificulta el

[38] Por ejemplo, la falta de información financiera también implica un mayor costo transaccional para remesas y pagos, aspecto extremadamente relevante para las familias de migrantes que viven en estos barrios.

[39] El GCBA está trabajando con el barrio en la titulación de estas propiedades.

acceso al mercado laboral formal por la imposibilidad de demostrar su trayectoria (BID, 2018).

Descripción de la solución

BID Lab, en conjunto con la Asociación Civil para el Desarrollo de Ecosistemas Descentralizados, está implementando un proyecto cuyo objetivo es desarrollar una identidad digital para habitantes de barrios vulnerables del Área Metropolitana de Buenos Aires a través de la tecnología *blockchain*, que facilite su acceso a bienes y servicios de calidad y promueva su inclusión financiera.

El proyecto considera que la identidad digital es un pilar crítico en la inclusión de población vulnerable. La tecnología habilitará un modelo de tipo soberano en el que las personas se apropien de su identidad –la cual será construida a partir de datos validados por terceras partes– y, por ende, estén en control de su información personal. Se propone utilizar la tecnología *blockchain* debido a sus atributos de inmutabilidad, transparencia y portabilidad (BID, 2018).

En esta prueba piloto la identidad digital de los habitantes del barrio se construirá a partir de varias fuentes. En primer lugar, a través de información generada por la implementación de una billetera digital para personas no bancarizadas, que permitirá el acceso a servicios financieros como atesoramiento de dinero digital, pagos, transferencias y remesas. Además de ofrecer una solución segura para el manejo de dinero digital, esta billetera permitirá a las personas ir construyendo un historial de transacciones, que serán la base de la información para habilitar su inclusión en el sistema financiero formal. Habiéndose realizado un proceso colaborativo de diagnóstico junto con los habitantes del barrio para identificar las necesidades de los distintos usuarios de la aplicación, en la actualidad se encuentran en etapa de desarrollo la plataforma de identidad digital y su billetera digital asociada. Se estima que el lanzamiento del prototipo se realizará a fines de 2019.

Para la implementación del prototipo se realizarán campañas de difusión y adopción, las que contarán con el trabajo de promotores que acompañarán a la población en el uso de la aplicación. Los promotores también serán responsables de relevar las experiencias, recibir eventuales reclamos de los usuarios y detectar posibles ajustes y mejoras a la aplicación. Un aspecto importante del proyecto es su compromiso con la reducción de la brecha digital de la población del barrio. A fin de promover la inclusión digital y la educación financiera, se realizarán capacitaciones de alfabetismo digital, educación financiera y emprendedurismo (BID, 2018).

En segundo lugar, el proyecto explorará la forma en que puede usarse *blockchain* para registrar la propiedad de los activos con que cuentan los habitantes en asentamientos informales como un plano adicional de información para nutrir la identidad digital. En este sentido, se buscará articular con las entidades públicas competentes, en el Barrio 31 y en otros barrios donde se implemente el piloto, la posibilidad de otorgar certificados de vivienda registrados en *blockchain*.

Finalmente, se buscará generar articulaciones y acuerdos con distintas entidades públicas y privadas que poseen información sobre la identidad de las personas (GCBA, empresas telefónicas, bancos, sector público, instituciones microfinancieras, supermercados, academias, etc.) para poder nutrir la identidad digital con más información. Es importante aclarar que la información que se comparta a través de la aplicación será propiedad del individuo, quien será el único que tendrá acceso a la totalidad de sus datos con su clave privada (BID, 2018). De esta forma se espera que las personas habitantes en barrios vulnerables pasen a tener el control de la información sobre su identidad y puedan usarla para acceder a bienes y servicios en igualdad de condiciones que el resto de la población.

El proyecto permitirá generar una identidad digital soberana para fomentar la inclusión social, cívica y económica a personas en situación de vulnerabilidad. El uso de *blockchain* para este caso particular permite recopilar e intercambiar pruebas de su identidad de diversas fuentes de forma segura y con la confianza de que los datos no han sido manipulados. Adicionalmente, permite que las personas se apropien de su identidad y, por ende, estén en control de su información personal y del valor que esta genera.

A través de la interoperabilidad generada por la existencia de una billetera que recopila toda la información del usuario, la tecnología tiene el potencial de aumentar la resistencia de los sistemas y la seguridad del almacenamiento de los datos debido a su naturaleza distribuida y la inexistencia de un punto central de control, sin la necesidad de construir una gran base de datos centralizada y vulnerable.

En particular, el proyecto permitirá: (i) certificar el origen de los datos presentados por los individuos y eliminar el riesgo de su adulteración, (ii) preservar la privacidad de los individuos, pero empoderarlos con información sobre su identidad, incluidos sus historiales transaccionales, (iii) permitir el acce-

so a mejores condiciones crediticias al mostrar un más amplio perfil, (iv) habilitar la tokenización de certificados de propiedad, vivienda, trabajo y méritos académicos, (v) facilitar la trazabilidad de activos formales e informales, y (vi) permitir transacciones a menor costo eliminando intermediarios y reduciendo tiempos y riesgos.

Consideraciones para una solución basada en *blockchain*

Las discusiones iniciales sobre cómo usar *blockchain* como plataforma para la identidad digital se centraron en la idea de almacenar datos personales directamente en la red. Sin embargo, rápidamente quedó claro que hacerlo generaría riesgos significativos de ciberseguridad y enfrentaría fuertes obstáculos regulatorios vinculados a la privacidad de los datos. Por esta razón, es importante identificar qué información se almacena en la cadena de bloques, ya que no es aconsejable almacenar datos sensibles. Los pilotos actuales utilizan modelos en los que las personas usan una billetera digital vinculada a una cadena de bloques que almacena certificaciones emitidas por autoridades de confianza[40] que afirman que las personas poseen ciertos atributos (Pisa y Juden, 2017), en lugar de almacenar información personal.

Otra consideración en la construcción de una identidad digital es la inclusión del gobierno en los pilotos desarrollados, ya que cuentan con información clave del usuario que permite identificar a la persona en un entorno digital. Asimismo, se necesita generar un ecosistema digital que utilice esta información para proveer servicios públicos y privados, de manera tal de generar los incentivos adecuados para fomentar su utilización; si esos servicios solo satisfacen una pequeña porción de las necesidades de identificación de una persona, entonces el valor de una identidad controlada por el usuario es limitado (Pisa y Juden, 2017).

Por último, este caso pone en evidencia la necesidad de generar habilidades digitales en los usuarios para poder hacer uso de la billetera y construir un ecosistema que genere y utilice información de las personas para proveer servicios de calidad. De esta manera, se democratiza el uso de la tecnología y se diseñan soluciones con base en el usuario y sus necesidades.

[40] Este modelo sugiere que los datos sensibles serán almacenados en un lugar seguro y solamente las certificaciones de atributos o afirmaciones específicas están transferidas en la cadena de bloques.

Otras tecnologías

La construcción de una identidad digital soberana puede realizarse a través de una plataforma de interoperabilidad con una PKI, que integre a todos los actores que poseen información valiosa de las personas en el sector público y en el privado. Sin embargo, teniendo en cuenta la diversidad de actores que conformarían el ecosistema que se quiere construir, los costos de coordinación y de adopción de estándares que pueden requerir desarrollos específicos podrían ser muy altos. La utilización de una solución basada en *blockchain* puede simplificar la necesidad de modificaciones en los sistemas existentes.

Reflexiones del caso

Este caso demuestra que *blockchain* tiene el potencial de crear una identidad digital para las personas sin la necesidad de que las bases de datos de los organismos que alojan atributos operen entre sí. De esta manera, se reducen costos en la implementación de una arquitectura tecnológica para que estas bases operen entre sí (ya que pasan a afirmar datos sobre los ciudadanos, los cuales se alojan en la billetera), aumentando la seguridad de la información y la autenticación.

Además, la tecnología permite la implementación de un modelo de tipo soberano que brinda la flexibilidad de recopilar e intercambiar pruebas de su identidad de diversas fuentes, eliminando así la dependencia de una autoridad centralizada. Lo innovador de esta solución es que por diseño las personas podrán apropiarse de su identidad, ejerciendo el control sobre sus datos personales y utilizando las afirmaciones de identidad para realizar transacciones.

Recuadro 4

La construcción de una identidad digital como pilar de la mejora de servicios

En 2001 el gobierno del estado de Illinois en los Estados Unidos desplegó la PKI para facilitar la certificación de documentos legales digitales por las agencias, juntas, comisiones, universidades, gobierno municipal y socios comerciales del estado de Illinois, ayudando a determinar la identidad de diferentes personas, dispositivos y servicios. A pesar de los beneficios incrementales que la infraestructura de clave pública ofrece a los servicios del gobierno, no se puede ver como una solución de seguridad de todos los datos y gestión de la identidad, sino que es una pieza del rompecabezas. Los datos que conforman la identidad de los ciudadanos a menudo están almacenados en bases de datos estatales en todas las agencias, lo que aumenta las posibilidades de fraude, violaciones de seguridad y errores (Morris, Mirkovic y O'Rourke, 2018).

Illinois sigue un enfoque proactivo en identificar el potencial de nuevas tecnologías para el ámbito público, que adapte sus servicios a las necesidades de las personas. Un estudio realizado en 2017 por el equipo de trabajo Illinois Blockchain and Distributed Ledger Task Force ha analizado el potencial de la tecnología *blockchain* para mejorar los procesos económicos y públicos. Según este estudio, la tecnología puede conectar entidades dispares dentro y entre entidades regionales, municipales y estatales en torno a ciudadanos, empresas y activos (Morris, Mirkovic y O'Rourke, 2018). El estudio sugiere que hay múltiples ventajas al establecer un ecosistema de identidad digital usando la tecnología *blockchain*, donde el gobierno desempeña un rol fundamental como gestor de los datos personales y proveedor de servicios.

Para hacer el manejo de la identidad digital más flexible, el estado de Illinois decidió implementar un piloto de una solución de infraestructura descentralizada de clave pública (DPKI) basada en la tecnología *blockchain*. La infraestructura DPKI aprovecha los bloques como un almacén de valores y se considera una forma más flexible de gestionar la infraestructura de clave pública (Morris, Mirkovic y O'Rourke, 2018). Los elementos centrales del piloto de solución de identidad digital basada en la tecnología *blockchain* son los siguientes:

I Cartera de atributos del ciudadano: los identificadores descentralizados en una cadena de bloques y las afirmaciones verificables se pueden usar para formar la base de la identidad de un ciudadano.

II Atributos de identidad y anexos: cada agencia gubernamental puede verificar y agregar nuevos atributos de identidad firmados criptográficamente a la billetera digital de un ciudadano. En este modelo, la billetera sería administrada por el usuario o un proveedor de servicios, mientras que la integridad de los atributos es mantenida por la entidad gubernamental.

III Registros de activos y propiedad: bajo esta arquitectura, para los activos y la propiedad también se pueden emitir identificadores descentralizados y atributos. Un título de propiedad o vehículo pueden representarse como un atributo y agregarse a la billetera de un ciudadano.

En este modelo el gobierno se convertiría en el verificador más que en el custodio de la identidad de las personas. Los datos personales encriptados y almacenados a través de esta arquitectura agregan seguridad, ya que se acceden a través de las claves privadas en manos de los ciudadanos que sirven para desbloquear los datos almacenados en su dispositivo personal. Las personas a su vez pueden compartir selectivamente los atributos verificados de su identidad y así proteger su privacidad (Morris, Mirkovic y O'Rourke, 2018).

III

¿Qué es *blockchain*?

3.1.
Definición y funcionamiento

Inicialmente introducida como la tecnología detrás de la criptomoneda Bitcoin,[41] la tecnología de cadena de bloques tiene potenciales usos que trascienden su aplicación original. Para definir *blockchain* se utilizará la definición del Instituto Nacional de Normas y Tecnología de los Estados Unidos:

Las cadenas de bloque (blockchain) son registros digitales distribuidos de transacciones firmadas criptográficamente que están agrupadas en bloques. Cada bloque está vinculado de manera criptográfica con el anterior después de una validación y una decisión de consenso. A medida que se agregan nuevos bloques, los bloques previos son más difíciles de cambiar. Los nuevos bloques son replicados en todas las copias del registro dentro de la red, y cualquier conflicto se resuelve automáticamente usando reglas establecidas. (Yaga et al., 2018).

Una explicación sobre cómo funciona *blockchain* puede ayudar a entender mejor esta definición.[42] Para exponer su funcionamiento, es bueno plantear primero el problema que la tecnología pretende resolver. El problema original que se plantea en la nota que propuso esta tecnología[43] es la imposibilidad de que dos personas puedan realizar una transacción de pago electrónico sin la participación de una tercera persona de confianza. Es decir: ¿cómo puede la persona que recibe el pago electrónico *saber* que la persona que realiza el pago cuenta con los recursos suficientes para realizarlo? Esta pregunta usualmente la responde un banco o una plataforma de pagos intermediaria pero, según el autor de la nota, estas entidades introducen barreras y costos para un libre mercado de pagos electrónicos. Entonces, la pregunta que surge es: ¿cómo deshacerse de ellos?

[41] Curiosamente, el término *blockchain* no fue incluido en el trabajo original que describe Bitcoin, de manera que algunos analistas sostienen que no existe aún una definición exacta de lo que es *blockchain*.

[42] Sin embargo, para una descripción más detallada de cómo funciona *blockchain*, se recomienda la publicación de Allende López (2018).

[43] Haber y Stornetta fueron los primeros en plantear este problema (el documento está disponible en: *https://www.anf.es/pdf/Haber_Stornetta.pdf*), que luego fue retomado por Satoshi Nakamoto en: Bitcoin: A Peer-to-Peer Electronic Cash System, publicado en 2008 (disponible en: *https://bitcoin.org/bitcoin.pdf*).

La primera parte de la respuesta pasa por la creación de una cadena de transacciones para cada participante de manera que se pueda conocer en todo momento el saldo monetario que cada persona tiene. Esto equivaldría a que cada billetera pudiese rastrear la cantidad de dinero que hubo en su interior desde que fue comprada. La suma de cuánto dinero entró a la billetera menos la suma de cuánto salió de ella debería (i) ser un número igual o mayor a cero, y (ii) ser igual a la cantidad de dinero que hay en la billetera en este momento. Este número es el máximo que se puede gastar. Entonces, si el propietario de la billetera quisiera engañar a alguien y gastar dinero que en realidad no tiene, debería de alguna manera alterar la historia de sus transacciones para aumentar la entrada de dinero y/o reducir alguna salida de dinero. ¿Cómo evitar entonces que alguien cambie la información histórica que determina el balance actual? En *blockchain* esto se puede hacer gracias al proceso de encadenamiento.

3.1.1. El proceso de encadenamiento

Para entender el proceso de encadenamiento, es importante conocer el concepto de *hasheado*. Este término se usa para describir el uso de funciones llamadas *hash*, las cuales utilizan un algoritmo para convertir cualquier texto, documento o información en una sucesión de caracteres (a la que se denomina *hash*) siempre de la misma extensión. El algoritmo es tal que, ante cualquier cambio en el texto o documento, se genera una sucesión de caracteres distinta. Por ejemplo, utilizando el algoritmo de la función SHA-256[44] sobre la primera oración de este párrafo, se genera la siguiente sucesión de caracteres[45] (véase el esquema 1):

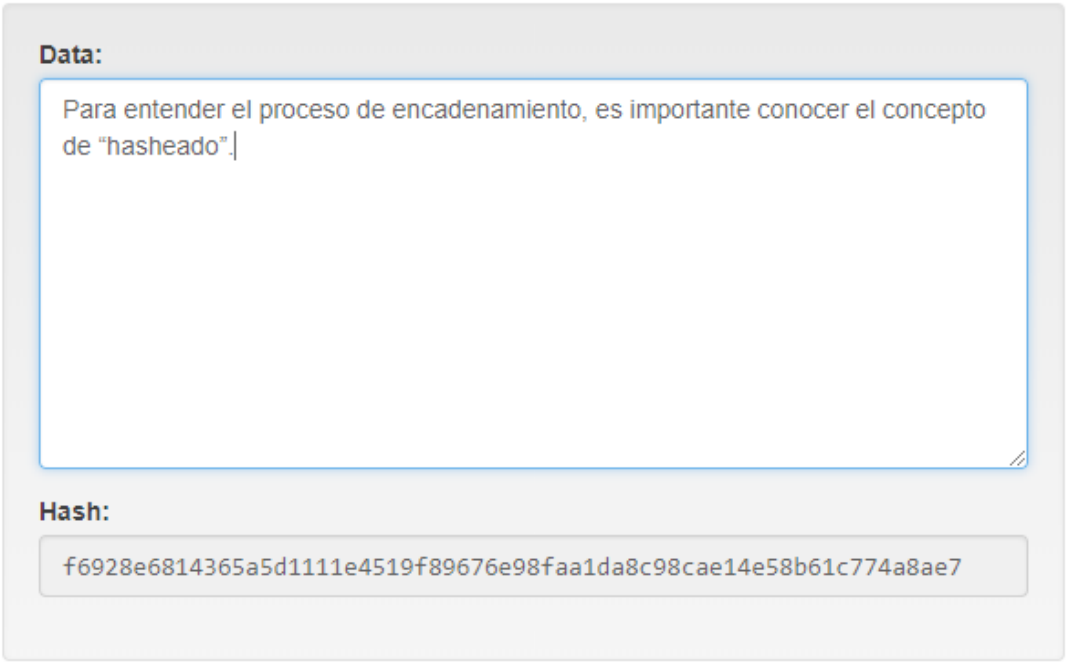
f6928e6814365a5d1111e4519f8 9676e98faa1da8c-98cae14e58b61c774a8ae7

Es importante notar dos cosas con respecto al uso de funciones *hash*: (i) es computacionalmente imposible cambiar alguna información en el texto original y que se genere el mismo *hash*; y (ii) la única forma de llegar a deducir el texto original desde la función *hash* es a través de prueba y error –fuerza bruta–, lo cual, dependiendo del tipo de función *hash* y la capacidad computacional que se tenga a disposición, podría llevar mucho tiempo porque implica probar todos los posibles *hashes* hasta encontrar el válido sin ninguna técnica que permita descartar a algunos de antemano.

[44] Este es el mismo algoritmo sugerido por Satoshi Nakamoto, pero existen otros disponibles.

[45] Para las demostraciones de la función *hash* se ha utilizado la demostración que Anders Brownworth ha incluido en *https://anders.com/blockchain/.*

Esquema 1. **Uso de la función *hash***



Entonces, ¿cómo funciona el encadenamiento en *blockchain*? Básicamente, en el caso de la *blockchain* detrás de Bitcoin, cada cierto número de transacciones[46] se crea un nuevo bloque, en el cual se incluye el *hash* del bloque anterior para crear un nuevo *hash* que corresponde al nuevo bloque. Es decir, cada nuevo bloque incluye el *hash* del bloque anterior, lo cual crea en la práctica una cadena de bloques que impide cambiar información contenida en un bloque anterior sin "arrastrar" cambios en los *hashes* de los bloques siguientes. Entonces, siguiendo el ejemplo de la billetera, todas las entradas y salidas de dinero de la billetera están encadenadas entre ellas de manera que cualquier intento de cambiar una transacción pasada genera un error a la hora de revisar el saldo actual.

Ahora bien, si esta cadena de bloques existiera en una sola computadora sería posible alterar la información, ya que al existir solo una copia el único "dueño" de la cadena podría cambiarla toda cuando quisiera.[47] Para evitar esto, entra en juego la segunda característica de *blockchain*: la distribución del registro.

[46] Cada transacción a su vez es firmada digitalmente por las partes.

[47] Se podrían argumentar algunas complicaciones que se vinculan con la firma digital que se genera cuando se agrega un nuevo bloque a la cadena y el registro de fecha y hora en el momento de la creación de un bloque, pero en general, si se trata de un registro único el administrador del mismo podrá modificarlo.

3.1.2. El registro distribuido

Esta característica simplemente trata de que el registro, es decir esa cadena de bloques que se va generando con cada nueva agrupación de información y que posee el *hash* del bloque anterior para garantizar que la información anterior no se ha cambiado, tenga una copia en varias computadoras, de hecho, en la mayor cantidad de computadoras posibles distribuidas en todo el mundo. Cada una de estas computadoras con una copia del registro tiene igual importancia que el resto; es decir: se trata de una red de pares en donde no existe alguien que domine al resto.

Ahora bien, para poder cambiar información en un bloque antiguo, habría que cambiar ese bloque y todos los bloques siguientes en todas las copias del registro, haciéndolo mucho más difícil. Más aún, teniendo en cuenta que el proceso *agrega* nuevos bloques continuamente, la labor de cambiar un bloque antiguo se convierte en casi imposible a medida que aumenta el número de bloques "encima" de aquel que se quiere cambiar, así como el número de copias del registro distribuidas en todo el mundo.

Lo que tendría que ocurrir para alterar una cadena de bloques es que alguien modificase una transacción en el bloque deseado y volviese a generar los *hashes* de ese bloque y el de los bloques siguientes coincidiesen con los *hashes* de la versión anterior de la cadena. Hacer esto es computacionalmente imposible para cada bloque, y ni siquiera se espera que la mecánica cuántica ofrezca una ventaja en este proceso (Allende López y Da Silva, 2019).

Sin embargo, esto genera una nueva pregunta: ¿qué pasa con la generación del siguiente bloque en un entorno de registros distribuidos donde todos tienen la misma importancia? ¿Quién se encarga de agregar un bloque adicional al registro y por qué se debe confiar en la veracidad de ese bloque? Es aquí donde cobra importancia el protocolo de consenso.

3.1.3. El protocolo de consenso

En un contexto de pares, ¿cómo se genera algún tipo de regla que permita agregar bloques de forma ordenada pero sin darle un poder adicional a alguno de los pares?, ¿cómo se llega a un consenso entre todas las partes respecto del siguiente bloque?, ¿cómo se genera un incentivo para que varios pares quieran agregar el siguiente bloque? El proceso para llegar a este consenso (llamado protocolo de consenso) en el caso de la *blockchain* de Bitcoin se llama prueba de trabajo o PoW (por sus siglas en inglés).

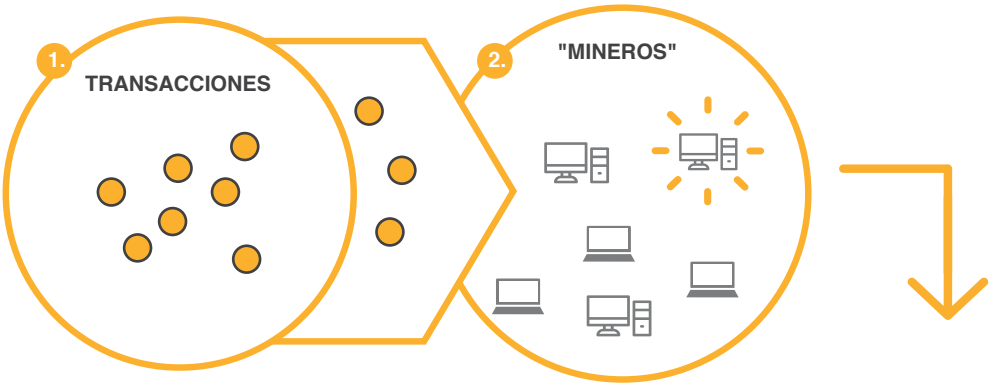
En resumen, el proceso es el siguiente: cada ente que quiere proponer un

nuevo bloque recoge la información que entraría en su bloque propuesto, agrega el *hash* del último bloque (que todos tienen en copia) y se dedica a resolver un problema matemático que en la práctica solo se puede resolver a través de prueba y error y que, por lo tanto, genera incentivos para una carrera basada casi exclusivamente en poseer la mayor capacidad computacional para resolver el problema.[48] Este proceso, llamado minería (de ahí que los participantes de esta competencia sean llamados mineros), tiene una recompensa que en el caso de la *blockchain* de Bitcoin consiste en un pago en Bitcoins y genera los incentivos para que más de un minero participe. El primero en resolver el problema transmite su nuevo bloque propuesto, incluyendo el *hash* de la cadena existente y la solución del problema matemático, al resto de los mineros, quienes deben validar la respuesta y, de estar correcta, agregar el nuevo bloque a su copia de la cadena. El proceso empieza nuevamente, ahora con un nuevo *hash* que incluye al bloque recientemente agregado.[49] El esquema 2 describe el proceso.

[48] Esta característica, si bien asegura cierta aleatoriedad en la selección del ente que propone el siguiente bloque, genera incentivos para el uso cada vez mayor de capacidad computacional y está detrás del excesivo consumo de energía de las *blockchain* públicas.

[49] En el caso de la *blockchain* de Bitcoin, el problema matemático se ajusta de manera que se genere un nuevo bloque cada 10 minutos aproximadamente.

ESQUEMA 2. CREACIÓN DE UN NUEVO BLOQUE



TRANSACCIÓN TRANSACCIÓN TRANSACCIÓN	TRANSACCIÓN TRANSACCIÓN TRANSACCIÓN	3. TRANSACCIÓN TRANSACCIÓN TRANSACCIÓN
FECHA Y HORA	FECHA Y HORA	FECHA Y HORA
HASH DE TRANSACCIONES	*HASH* DE TRANSACCIONES	*HASH* DE TRANSACCIONES
HASH BLOQUE (X - 1)	*HASH* BLOQUE X	*HASH* BLOQUE (X+1)
SOLUCIÓN AL PROBLEMA	SOLUCIÓN AL PROBLEMA	SOLUCIÓN AL PROBLEMA

1. Nuevas transacciones son enviadas a la red para ser validadas.

2. Los "mineros" conforme van recibiendo estas transacciones validan y reúnen para proponer nuevos bloques de la cadena. Para esto, las agregan, suman el *hash* del último bloque de la cadena y resuelven el problema matemático.

3. El primer "minero" en resolver el problema envía el bloque al resto de nodos. Estos validan la información del bloque y lo agregan como un nuevo bloque. El ciclo empieza de nuevo

Fuente: Elaboración propia con base en Allende López (2018) y Pisa y Juden (2017).

Entonces siguiendo el ejemplo de la billetera y el problema original que se planteó inicialmente, la tecnología *blockchain* genera un registro distribuido (todos tienen una copia) y encadenado (cada bloque contiene el *hash* del anterior) de transacciones que garantiza que el saldo de cada billetera sea el real. Nuevas transacciones son agregadas mediante un proceso que no le da privilegios a ninguna de las partes. En la práctica para aceptar una transacción incluida en un bloque, se espera que un número de bloques nuevos se escriba encima del que contiene la transacción de manera que sea muy difícil cambiarla.[50]

Es importante mencionar que el encadenamiento de información (la cadena propiamente dicha) no es una innovación ni es exclusiva de las criptomonedas. Como apunta Allende López (2018), se pueden encontrar menciones a la posibilidad de etiquetar y encadenar información desde 1991. Por otro lado, el copiar la información en varios sitios distintos para conservar la integridad de la información tampoco es novedad. La innovación más grande que introduce *blockchain* es la combinación de estas dos cosas junto con el protocolo de consenso,[51] todos los cuales permiten efectivamente prescindir de un tercero en quien confiar para agregar información segura en un registro.

Finalmente, hay una característica del protocolo de consenso que usa la *blockchain* de Bitcoin que aún no se ha mencionado: su excesivo consumo de energía. La manera en la que se ha definido el proceso de minado es tal que cada 10 minutos (aproximadamente) se agrega un nuevo bloque a la cadena. Ahora bien, debido a la naturaleza del problema matemático que determina quién agregará el siguiente bloque, los mineros que compiten por hacerlo tienen incentivos para invertir en mayor capacidad computacional para ser los primeros en resolver el problema. Como cada nuevo bloque debe agregarse cada 10 minutos y ante el incremento en capacidad computacional de los mineros, el problema matemático se vuelve cada vez más difícil, lo cual genera un círculo vicioso de inversión en capacidad computacional y un consumo descomunal de energía que se anticipa solo crecerá.[52]

[50] Teóricamente, si algún agente controla el 50% + 1 de los nodos podría forzar una nueva cadena con transacciones fraudulentas. A este tipo de ataque se le denomina ataque del 51%. El pedir confirmaciones o un número de bloques posteriores al registro de la transacción ayudan a reducir la probabilidad de éxito de este tipo de ataques. En la práctica (por lo menos en la *blockchain* de Bitcoin) un ataque de este tipo requiere de una inversión en capacidad computacional que excede los potenciales beneficios que podrían obtenerse.

[51] Más información disponible en: *http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf*.

[52] Según *The Economist*, se estima que durante 2018 los mineros de *blockchain* consumirán energía equivalente a la de todo Irlanda (puede leerse la nota completa en: *https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy)*.

3.2.
Tipos de *blockchain*

Hasta ahora se ha explicado el funcionamiento de las llamadas *blockchain* públicas no permisionadas. Estas son las que se derivan de la propuesta original de Satoshi Nakamoto, donde cualquier persona que es parte de la red puede ser un minero (si tiene la capacidad computacional requerida hoy en día), y puede acceder a todas las transacciones registradas en la cadena. Las *blockchain* públicas, no permisionadas más conocidas son la *blockchain* de Bitcoin y la de Ethereum, pero existen cientos de iniciativas (la mayoría ligadas a criptomonedas) que se basan en este tipo de *blockchain*. Si bien en esta publicación se ha descrito en detalle el protocolo de consenso que usan Bitcoin y Ethereum, existen otros que pueden aplicar las *blockchain* públicas, como la prueba de interés (PoS, por sus siglas en inglés). En todo caso, se trata de mecanismos que eligen de manera aleatoria al nodo que propone el siguiente bloque en la cadena y a la vez generan incentivos para que haya varios/muchos nodos interesados en hacerlo.

Pero existen también las llamadas *blockchain* permisionadas, tanto públicas como privadas. La principal diferencia entre *blockchain* no permisionadas y las permisionadas es que en el caso de las segundas se necesita autorización para participar. En estos casos el protocolo de consenso también se aleja del PoW explicado en la sección anterior. En su reemplazo, se crean otras reglas de consenso que, dependiendo del tipo de aplicación particular, pueden eliminar la igualdad de pares que la *blockchain* pública tiene o incluso introducir la necesidad de confiar en alguno(s) de los participantes.[53]

Es importante resaltar que debido al menor número de participantes las *blockchain* permisionadas-privadas no ofrecen el mismo nivel de seguridad e inmutabilidad de los datos que las *blockchain* públicas. El uso de protocolos de consenso distintos al PoW en las *blockchain* permisionadas afecta la simetría entre pares y la eliminación de la necesidad de confianza entre las mismas. Sin embargo, como se ha visto antes, el valor de las redes privadas permisionadas reside en la facilidad para el intercambio de información más que en la integridad de la información o la falta de necesidad de confianza en un tercero. El esquema 3, desarrollado originalmente por McKinsey (2018), muestra las principales diferencias entre los distintos tipos de *blockchain.*

[53] Una de las reglas más usadas se basa en la adaptación de la solución al problema de los generales bizantinos, también llamado consenso bizantino o protocolo bizantino. Más información disponible en: *https://es.wikipedia.org/wiki/Problema_de_los_generales_bizantinos*.

ESQUEMA 3. ***BLOCKCHAIN*: OPCIONES DE ARQUITECTURA**

		Arquitectura basada en permisos para que los participantes puedan unirse, leer o agregar bloques	
		NO PERMISIONADA	**PERMISIONADA**
Arquitectura basada en la propiedad de la infrastructura de datos	**PÚBLICA**	• Cualquiera puede unirse, leer y agregar bloques • Alojado en servidores públicos • Anónimo y altamente resiliente • Baja escalabilidad	• Cualquiera puede unirse y leer • Solo participantes autorizados y conocidos pueden agregar bloques • Escalabilidad media
	PRIVADA	• Solo participantes autorizados pueden unirse, leer y escribir • Alojado en servidores privados • Altamente escalable	• Solo participantes autorizados pueden unirse y leer • Solo operador de la red puede agregar bloques • Muy escalable

Fuente: McKinsey (2018).

3.3.
Contratos inteligentes

Sin importar el tipo de *blockchain*, uno de los principales usos potenciales de la tecnología es la posibilidad de escribir algoritmos (procesos, condiciones, acciones) en un bloque, los cuales se ejecutarán cuando se cumpla(n) alguna(s) condiciones preestablecidas. A estos algoritmos se los llama contratos inteligentes. Desde la realización de transferencias financieras periódicas hasta pagos una vez confirmado un envío, el potencial de los contratos inteligentes es alto. Una vez escrito el código y firmado digitalmente a la hora de agregarlo a la cadena de bloques, su ejecución (cuando se cumpla alguna condición establecida o se realice la activación del mismo a través de un pago) es realizada –y corroborada– por todos los participantes de la red.

Si bien puede haber un alto potencial detrás del uso de contratos inteligentes existen algunos puntos a considerar. El primero es que, efectivamente, una vez escritos los contratos en *blockchain*, estos quedarán inscritos en la cadena de bloques como cualquier otra información. Es decir: no podrá cambiarse ni podrá terminarse, a menos que el contrato mismo incluya alguna condición para hacerlo. En segundo lugar, cualquier pago o transferencia vinculados a esta transacción se podrán realizar dentro del mismo ámbito de la cadena. Es decir, para las redes permisionadas basadas en criptomonedas, la mayoría de los pagos y transferencias será en la criptomoneda que la cadena de bloques soporte. En el caso de las redes no permisionadas a fin de disponer dinero virtual para realizar transacciones, este se debe tokenizar; este dinero tokenizado permite poder comprar y vender activos.[54] Finalmente, es importante mencionar que cualquier falla en el código del contrato puede tener consecuencias no anticipadas, desde la posibilidad de fraude por parte de programadores que explotan alguna debilidad en el código hasta el estancamiento de dinero por alguna falla en el código que, por ejemplo, reduzca el balance de una cuenta pero no aumente el de ninguna otra.

[54] Depender de un tercero para realizar la transferencia o pago en la práctica puede anular buena parte de la propuesta de valor por la cual se usó la cadena de bloques en primer lugar.

3.4.
Tokenización de activos

Hasta ahora se han mencionado las transacciones monetarias escritas y transferidas en la *blockchain*. Las sumas y restas de las billeteras tenían la misma unidad de medida y lo importante es la verificación del saldo final. Sin embargo, se podría reemplazar la moneda por distintas fichas (*tokens*), cada una de las cuales representa un activo distinto (una parte o la totalidad de un activo, físico o virtual, por ejemplo). Así, lo importante ya no será el saldo al final de todas las transacciones sino cada transacción de manera individual, ya que cada una es una representación en *blockchain* de un cambio (transferencia de propiedad, por ejemplo) de algún activo.

3.5.
Time stamping

Cuando se valida una transacción y se agrega a un bloque en la cadena, esta validación incluirá la hora exacta de la transacción y la firma digital de quien la haya enviado. Esta verificación de la fecha y hora de una transacción, llamada *time stamping*, puede a veces ser muy valiosa en sí misma porque puede servir para demostrar el momento en que una acción específica ocurrió. La consistencia en la información entre todos los nodos participantes minimiza la probabilidad de manipulación y otorga un alto grado de certeza respecto del momento en el que se realizó la transacción.

3.6.
Atributos de *blockchain*

El cuadro 2 recoge los principales atributos y beneficios que ofrece la tecnología *blockchain* en función de lo presentado anteriormente. Es importante notar que, como se ha explicado, el uso de una *blockchain* privada (o federada) afecta el alcance de algunos atributos, los cuales dependerán en estos casos del protocolo de consenso que se utilice, del número de nodos que sean parte de la red y del grado de independencia de los nodos. Finalmente, también es importante mencionar que la inmutabilidad de la información en *blockchain* es producto de varios atributos: (i) la distribución en tiempo casi real, (ii) el encadenamiento y (iii) el mecanismo de consenso. Sin embargo, cabe destacar que el grado de inmutabilidad de la información es directamente proporcional al número de nodos independientes que existan en la red.

CUADRO 2. ATRIBUTOS DE *BLOCKCHAIN*

ATRIBUTO	BENEFICIO	DESCRIPCIÓN	CONSIDERACIONES
Distribución en tiempo casi real	Consistencia en la información entre todos los nodos	La información es copiada automáticamente en múltiples nodos en tiempo casi real como parte del protocolo de consenso.	En redes públicas, el consenso (proceso para registrar un nuevo bloque en la cadena) demora alrededor de 10 minutos,[a] pudiendo llegar a una hora dependiendo del número de confirmaciones que se requiera.
Lectura	Transparencia	Todos los participantes pueden acceder a la información de la *blockchain*.	En redes privadas se puede restringir el acceso a cierto tipo de usuarios.
Escritura	Acceso extendido	Todos los participantes pueden agregar información a la *blockchain*.	En redes privadas se puede restringir el acceso a cierto tipo de usuarios (distinto al que tiene acceso de lectura).
Encadenamiento	Seguridad en la trazabilidad	No se puede editar ni borrar un bloque, solo se puede agregar uno nuevo	Dependiendo del protocolo de consenso, los bloques se pueden cambiar si el 50% + 1 de nodos se coluden. En redes privadas, dependiendo del número de nodos, esto puede ser más fácil.
Protocolo de consenso	Prescindir del intermediario de confianza	Proceso para agregar nuevos bloques a la cadena sin necesidad de un intermediario o entidad de validación. El PoW es el más conocido y usado.	El PoW retrasa el registro de transacciones y consume mucha energía. En redes privadas se puede tener más flexibilidad para validar transacciones, incluyendo a uno o varios intermediarios. Sin embargo, en estos casos se termina creando una estructura de confianza en alguno(s) de los participantes.
Firma digital y encriptación	Seguridad de la información, *time stamping*	La información que se agrega a la cadena es firmada digitalmente y encriptada.	Cada usuario tiene credenciales para escribir en la cadena. En redes privadas es posible que se necesiten credenciales para leer también. Con el tiempo y los avances tecnológicos, la encriptación puede ser superada, por lo que hay que pensar muy bien el tipo de información a incluir en la cadena de bloques.
Contratos inteligentes	Certidumbre y reglas claras	Algoritmos incluidos en la *blockchain* con reglas que se activan cuando se cumplen ciertos criterios predefinidos.	En general, el código deber ser auditado minuciosamente, en particular en aquellos contratos que incluyan condiciones complejas o involucren grandes cantidades de dinero. La interfaz con el mundo externo en muchos casos igual requiere de un tercero de confianza (oráculo).

Nota: [a]. Este tiempo se calcula utilizando la POW, que es el protocolo de consenso detrás de Bitcoin y Ethereum, las plataformas de *blockchain* públicas más utilizadas.

Siguientes pasos: menos ruido y más bloques

Blockchain es una tecnología tan nueva que aún no existe una definición aceptada por todos. Por un lado, es cierto que la tecnología ofrece varios atributos que podrían ser de interés de la administración pública. Por otro, se trata probablemente de una de las maneras más costosas de guardar información.

En este sentido, es importante entender las limitaciones de la tecnología, así como los casos en los que estos beneficios se vulneran o desaparecen. Por ejemplo, la falta de confianza entre las partes podría desaparecer con una red privada y/o permisionada, la cual necesita de un nivel de confianza entre participantes, ya que estas redes pueden disminuir el grado de dificultad de cambiar información escrita en la cadena al tener un número menor de nodos y/o protocolos de consenso distintos al de las redes públicas no permisionadas.

Se han identificado cuatro espacios donde se considera que la tecnología puede apoyar a la administración pública mejorando o haciendo más efectiva la prestación de servicios públicos:

I Desintermediación de la información.
II Tokenización de activos.
III Automatización de procesos.
IV Interoperabilidad en el borde.

Para cada una de estas funciones, en la segunda parte se explica el rol que la tecnología podría desempeñar, se exponen proyectos y se trata de comparar *blockchain* con alguna otra tecnología que podría realizar esa función. También en la primera parte se presenta una lista de consideraciones que hay que tener en cuenta para pasar de proyectos a iniciativas escalables.

En el futuro, es importante que a medida que se pase de una modalidad de aprendizaje a una de aplicación de la tecnología se priorice el problema que se quiere resolver por encima de cualquier tecnología específica. En ese sentido, se recomienda revisar los Principios Digitales,[55] recientemente adoptados por el BID, como una guía general del uso de tecnología en proyectos de desarrollo.

En particular, se considera que las siguientes acciones pueden ayudar a las administraciones públicas que quieren continuar experimentando con la tecnología.

[55] Más información disponible en: *https://digitalprinciples.org/*.

Formalizar la creación de un espacio para la experimentación

La formalización de una iniciativa para experimentar con nuevas tecnologías (incluyendo *blockchain*) genera el espacio para que un equipo del gobierno explore con más facilidad los atributos de las distintas tecnologías, así como sus potenciales usos. Países como Estados Unidos, India y Singapur ya han establecido este tipo de cajas de arena (*sandbox*es) en el ámbito regulatorio, para analizar los impactos regulatorios detrás de las transacciones usando criptomonedas. La creación de un espacio más amplio para analizar y experimentar la tecnología podría también generar habilidades al interior de la administración pública que van a ser necesarias para poder administrar proyectos que utilicen la tecnología.

Diseñar para escalar

Uno de los principales problemas que se han observado es que muchas de las instancias de uso de la tecnología han sido diseñadas como un piloto aislado de los procesos y sistemas tradicionales, lo cual ha dificultado su escalamiento. El problema con este enfoque es que, incluso si la implementación es exitosa, no se puede escalar para un despliegue en producción. Cualquier proyecto con la ambición de convertirse en una iniciativa a nivel nacional debe diseñarse con este objetivo en mente, de manera que, una vez se demuestre su mérito y luego de una evaluación positiva en comparación con las tecnologías vigentes, su despliegue no requiera de un regreso a la etapa de diseño, que puede en sí misma introducir nuevas incertidumbres a la aplicación misma.

Tener un enfoque holístico tanto en la aplicación de la tecnología como en su evaluación

Desde un inicio, se debe tener en mente el ecosistema en el que se va a insertar la solución tecnológica. La selección de una tecnología debe producirse en función de la necesidad que se busca atender y no al revés. El proceso de identificación de problemas es independiente de las tecnologías (nuevas o existentes), y solo una vez conocido el problema se podrá pensar en las potenciales tecnologías para atenderlo. Asimismo, en el caso de las nuevas tecnologías se debe pensar en los aspectos regulatorios, los distintos actores que forman parte del servicio que se quiere implementar, el nivel de digitalización del servicio, etc., de manera de que no se tome el proyecto aislado de la realidad en la que va a tener que existir una vez desplegado.

Capacitar talento al interior de la administración pública

Si bien ya se mencionó antes, es una cuestión bastante importante: las nuevas tecnologías, en particular aquellas

que manipulan información personal, exigen al sector público un nivel mínimo de entendimiento de su funcionamiento para poder salvaguardar los derechos de los ciudadanos; estos, a su vez, necesitarían también comprender la tecnología para poder confiar en el uso que hace el gobierno de esos derechos. Existe un balance entre regulación y capacidad de innovación que debe ser constantemente revisado, y para eso se requiere de profesionales multidisciplinarios que estén al día con los avances tecnológicos y la regulación internacional.

Más allá de estas acciones concretas, esta publicación considera que en la medida en que la tecnología *blockchain* se vaya consolidando, los casos de uso que generan más valor para las administraciones públicas serán más claros. Probablemente aquellas administraciones que tengan un mejor entendimiento de la tecnología podrán ser los pioneros en su adopción.

REFERENCIAS

ACT-IAC (American Council for Technology and Industry Advisory Council). 2018. Blockchain Playbook Online - beta. Disponible en: https://blockchain-working-group.github.io/blockchain-playbook/intro/

AGESIC (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento). 2018. Blockchain Playbook: ¿Blockchain sí o no? Tecnologías Emergentes. Versión 2018.12.10

Allen, C. 2016. The Path to Self-Sovereign Identity. Disponible en: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Allende López, M. 2018. Blockchain: Cómo desarrollar confianza en entornos complejos para generar valor de impacto social. Washington, D.C.: BID. Disponible en: https://publications.iadb.org/handle/11319/8919.

Allende López, M. y M. M. Da Silva. 2019. Tecnologías cuánticas: Una oportunidad transversal e interdisciplinar para la transformación digital y el impacto social. Washington, D.C.: BID. Disponible en: https://publications.iadb.org/es/tecnologias-cuanticas-una-oportunidad-transversal-e-interdisciplinar-para-la-transformacion-digital

Allessie, D., M. Sobolewski, L. Vaccari y F. Pignatelli (Ed.). 2019. Blockchain for Digital Government. Luxemburgo: Oficina de Publicaciones de la Unión Europea.

BID (Banco Interamericano de Desarrollo). 2018. AR-T1190: inclusión social, cívica y económica de habitantes de barrios vulnerables en Buenos Aires mediante modelos de blockchain. Documento de proyecto. Disponible en: https://www.iadb.org/es/project/AR-T1190.

Berryhill, J., T. Bourgery y A. Hanson. 2018. Blockchains Unchained: Blockchain Technology and its Use in the Public Sector. Documento de trabajo de la OCDE sobre Gobernanza Pública, No. 28. París, Francia: OECD Publishing.

Bosankic, L. 2018. Blockchain Governance: Takeaways from Nine Projects. *Medium Blog*. Disponible en: https://medium.com/@leo_pold_b/blockchain-governance-takeaways-from-nine-projects-8a80ad214d15

Cepeda, J., A. De Luca, L. Jolías y D. Zelaya. 2017. Blockchain y transparencia: La experiencia en la ciudad de Bahía Blanca (Argentina). Fellowship OEA en Gobierno Abierto para las Américas.

CIDGE (Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico). 2017. Blockchain HACKMX. Reporte. SEFP-CEDN.

Consorcio Alastria. 2018. Alastria: Consorcio Nacional Multisectorial Blockchain. Presentación General. Disponible en: https://alastria.io/wp-content/uploads/2019/07/2019-07-11_Alastria-Presentaci%C3%B3n-corporativa_v00.10-2.pdf

DLA Piper. 2017. Blockchain: Background, Challenges, and Legal Issues. Disponible en: https://www.dlapiper.com/~/media/files/insights/publications/2017/06/blockchain_background_challenges_legal_issues_v6.pdf

Ehrsam, F. 2017. Blockchain Governance: Programming Our Future. *Medium Blog*. Disponible en: https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74

Exonum (n.d.). Improving the security of a government land registry: the case of National Agency of Public Registry in the Republic of Georgia. Disponible en: https://exonum.com/story-georgia

Friedman, S. 2017. GSA Looks to Blockchain for Speeding Procurement Processes. GCN. Disponible en: https://fcw.com/GIG/gcn/Articles/2017/09/21/GSA-looks-to-blockchain-for-procurement.aspx

Goldstein, P. 2018. Treasury, GSA See the Benefits of Blockchain. FedTech. Disponible en: https://fedtechmagazine.com/article/2018/01/treasury-gsa-see-benefits-blockchain

Graglia, M. 2017. Tbilisi Agreement Heralds Significant Expansion of Blockchain to Manage Property Registries. *New America Blog*. Disponible en: https://www.newamerica.org/international-security/future-property-rights/blog/blockchain-for-property-rights-georgia/

Graglia, J. M. y C. Mellon. 2018. Blockchain and Property in 2018: At the End of the Beginning. Documento preparado para ser presentado en 2018 World Bank Conference on Land and Poverty, Washington, D.C. Disponible en: https://www.newamerica.org/documents/2121/Graglia_Mellon_blockchain.pdf

GSA (Administración de Servicios Generales). 2017.GSA: Background and History. Disponible en: https://www.gsa.gov/about-us/background-and-history

GSMA, World Bank Group y Security Identity Alliance. 2016. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. Documento de trabajo. Disponible en: https://openknowledge.worldbank.org/handle/10986/24920

Hileman, G. y M. Rauchs. 2017. Global Blockchain Benchmarking Study. Cambridge, Reino Unido: Cambridge Center for Alternative Finance, University of Cambridge.

Jolías, L. 2018. Blockchain y compras públicas: la experiencia de Chile Compra. Chile Compra.

Kelman, S. 2017. GSA's Blockchain Blockbuster. FCW. Disponible en: https://fcw.com/blogs/lectern/2017/10/comment-kelman-gsa-blockchain.aspx

LACChain Alliance. 2019. ¿Qué es y en qué consiste la alianza global LACChain? *Medium Blog*. Disponible en: https://medium.com/@lacchain.official/qu%C3%A9-es-y-en-qu%C3%A9-consiste-la-alianza-global-lacchain-4d37f35d9746

Lewis, A. 2017. A Gentle Introduction to Self-sovereign Identity. Disponible en: https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/

Maecenas. 2018. Maecenas: The Decenstralised Art Gallery. White Paper. Disponible en: https://www.maecenas.co/

Mas, I. y D. Porteous. 2015. Identity and inclusion: When do digital identities help the poor? *Brookings Blog*. Disponible en: https://www.brookings.edu/blog/techtank/2015/03/10/identity-and-inclusion-when-do-digital-identities-help-the-poor/

McKinsey. 2018. Blockchain beyond the Hype: What is the Strategic Business Value? *McKinsey Digital*, junio. Disponible en: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

Morris, C., J. Mirkovic y J. M. O'Rourke. 2018. Final Report to the General Assembly. Illinois General Assembly Blockchain and Distributed Ledger Task Force. Disponible en: https://assets.documentcloud.org/documents/4368019/Blockchain-Task-Force-Final-Report-as-Filed.pdf

Nelson, P. 2018. Primer on Blockchain: How to Assess the Relevance of Distributed Ledger Technology to International Development. USAID.

OCDE (Organización para la Cooperación y el Desarrollo Económicos). 2018. Estudio del Sistema Electrónico de Contratación Pública de México: Rediseñando CompraNet de manera incluyente. Estudios de la OCDE sobre Gobernanza Pública. 9 de enero.

Pisa, M. 2018. Reassessing Expectations for Blockchain and Development. Center for Global Development Note. Disponible en: https://www.cgdev.org/sites/default/files/reassessing-expectations-blockchain-and-development-cost-complexity.pdf

Pisa, M. y M. Juden. 2017. Blockchain and Economic Development: Hype vs. Reality. Center for Global Development. Disponible en: https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality

Preukschat, A. 2018. Self-Sovereign Identity — a Guide to Privacy for Your Digital Identity with Blockchain. *Medium Blog*. Disponible en: https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-privacy-for-your-digital-identity-5b9e95677778

Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Disponible en: https://bitcoin.org/bitcoin.pdf

Thornton, D. 2017. GSA Experimenting with Blockchain to Cut Contracting Time. Federal News Network. Disponible en: https://federalnewsradio.com/it-modernization-2017/2017/11/gsa-experimenting-with-blockchain-to-cut-contracting-time/

Torregrossa, M. 2018. Blockchain for Public Servants: Everything You Need to Know. *Apolitical Blog*. Disponible en: https://apolitical.co/solution_article/blockchain-for-public-servants-everything-you-need-to-know/

UE (Unión Europea). 2018a. Blockchain for Government and Public Services. Thematic Report. UE Blockchain Observatory and Forum.

UE (Unión Europea). 2018b. Blockchain and the GPRD. Thematic Report. UE Blockchain Observatory and Forum.

Verhulst, S. 2018. Blockchain for Social Impact: Design Principles. *Apolitical Blog*. Disponible en: https://apolitical.co/solution_article/design-principles-blockchain-for-social-impact/

Voshmgir, S. 2017. Identity as a Bottleneck for Blockchain. Disponible en: https://stories.jolocom.com/identity-blockchain-the-road-to-self-sovereign-identity-f9f4439c52cb

Wachal, M. 2018. Asset Tokenization on Blockchain Will Disrupt the Asset Management Landscape. *Softwaremill Blog*. Disponible en: https://blog.softwaremill.com/asset-tokenization-on-blockchain-will-disrupt-the-asset-management-landscape-befbd71639b1

WEF (Foro Económico Mundial). 2016. A Blueprint for Digital Identity. Future of Financial Services Series. Agosto 2016. Disponible en: http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

WEF (Foro Económico Mundial). 2018. Blockchain Beyond the Hype: A Practical Framework for Business Leaders. WEF White Paper. Disponible en: http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf

Weiss, M. y E. Corsi. 2017. Bitfury: Blockchain for Government. Harvard Business School Case 818-031.

Wust, K. y A. Gervais. 2017. Do you need a Blockchain? Disponible en: https://eprint.iacr.org/2017/375.pdf

Yaga, D., P. Mell, N. Roby y K. Scarfone. 2018. Blockchain Technology Overview. NISTIR 8202 (DRAFT). NIST. Disponible en: https://csrc.nist.gov/publications/detail/nistir/8202/draft

Zambrano, R. 2018. Blockchain: Unpacking the Disruptive Potential of Blockchain Technology for Human Development. White Paper, IDRC.


BID