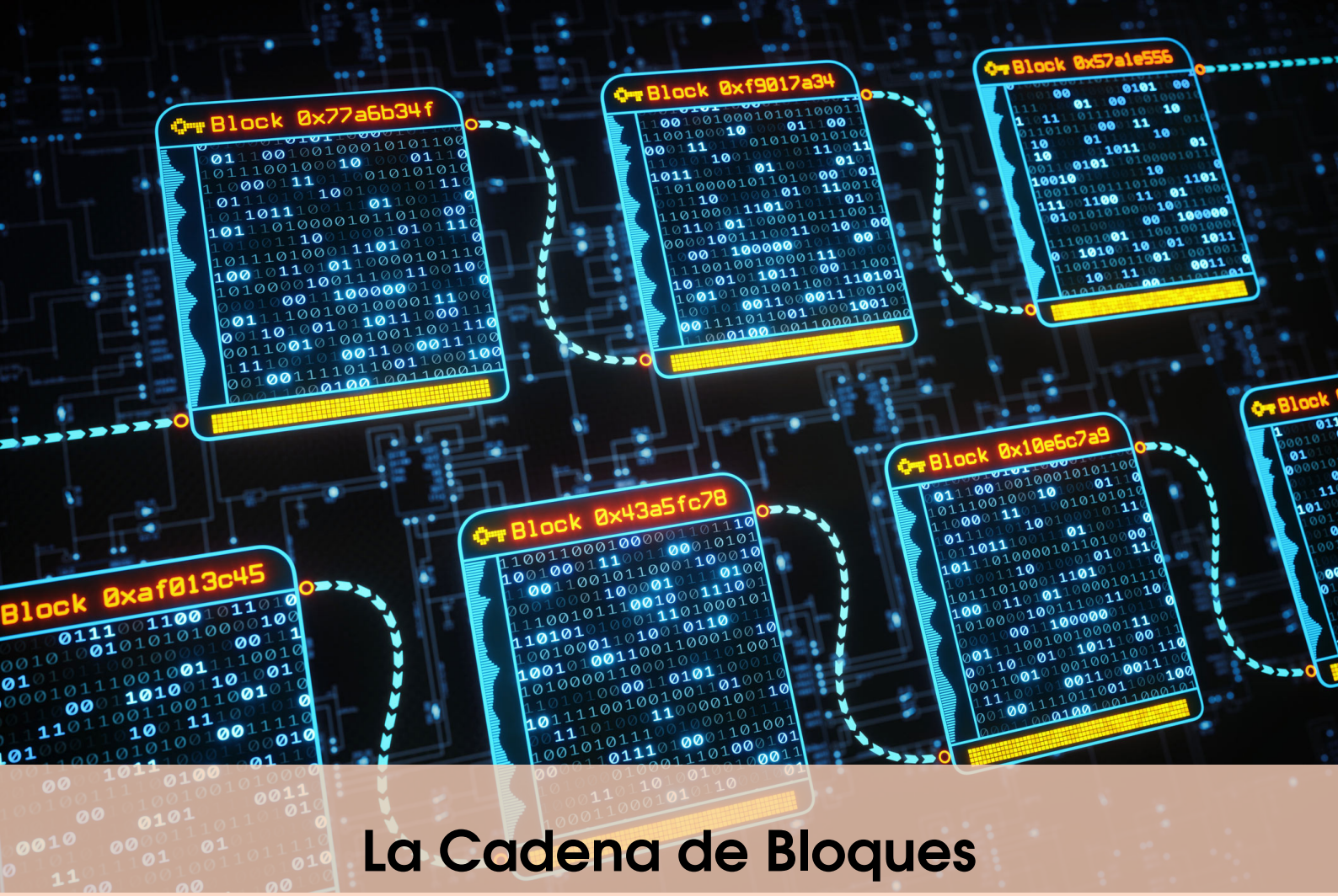


La Cadena de Bloques Blockchain

Un abordaje comprensible a su definición y posibles usos

Mg. Carlos Brys
Dirección de Modernización de la Gestión y Gobierno Electrónico
Subsecretaría de Coordinación y Relaciones Institucionales

Ministerio de Coordinación General de Gabinete

MISIONES
PROVINCIA

GOBIERNO DE LA PROVINCIA DE MISIONES

La Cadena de Bloques - Blockchain

Un abordaje comprensible a su definición y posibles usos

Mg. Carlos Brys

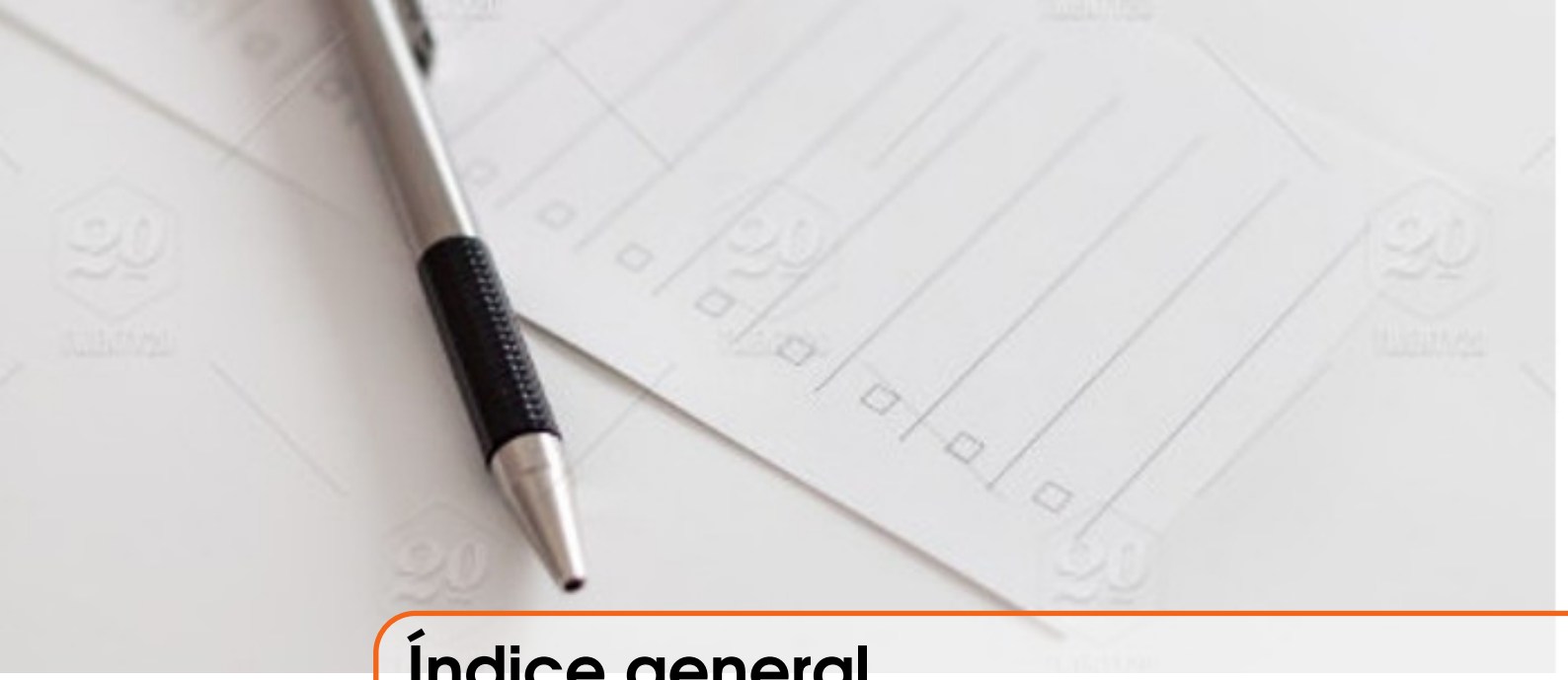
ELABORADO POR LA DIRECCIÓN DE MODERNIZACIÓN DE LA GESTIÓN Y GOBIERNO ELECTRÓNICO

Este texto fue escrito en LaTeX, un sistema de preparación de documentos libre.

Puede descargar ese documento de la siguiente dirección de Internet:

http://www.egov.misiones.gov.ar/index.php/biblioteca/informes/La-Cadena-de-Bloques/

Primera revisión, Enero 2019



Índice general

Conceptualización

1. Introducción

La tecnología de la **Cadena de Bloques** es una innovación tan profundamente disruptiva, que nos obligará a redefinir los conceptos y rediseñar completamente los procesos que rigen a la administración pública.

Se la considera como el quinto paradigma de la computación, después de la computadora personal, la Internet, la revolución de la tecnología móvil y la computación en la nube.

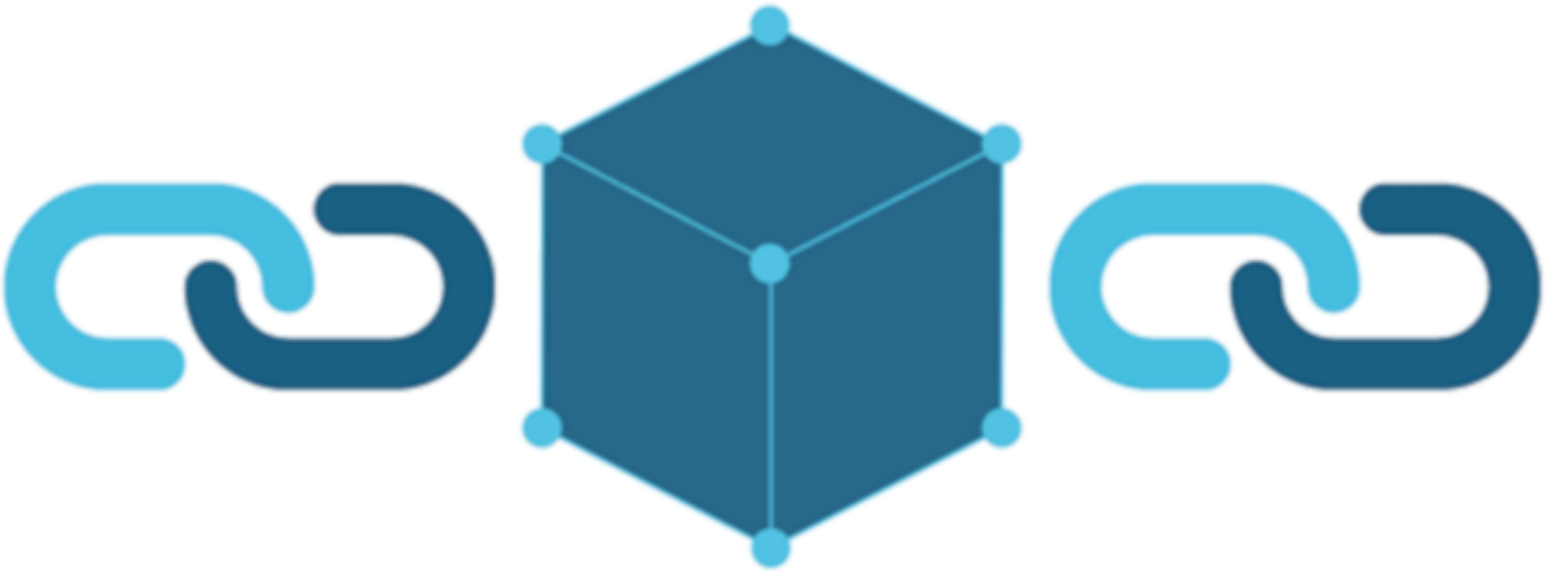
Debido a que es una tecnología sin precedentes, lograr su comprensión y aceptación por parte de los tomadores de decisiones, el ámbito político y legislativo, los desarrolladores de sistemas y los usuarios, constituye un reto que debe atenderse en lo inmediato.

La potencialidad de esta tecnología, a la que muchos de los investigadores la comparan con la creación de la Internet por el gran impacto que puede causar, es capaz de prescindir de la figura de una institución intermediaria certificante, que se encargue de guardar y validar los datos o información sobre los actos y los hechos.

Para considerar esta situación se requiere crear todo un nuevo paradigma de conocimiento y confianza hacia la tecnología que lo habilita y lo permite.

Creemos que esta tecnología, y como consecuencia de los profundos efectos que producirá en los sectores de servicios administrativos, requieren de una inmediata atención y comprensión.

En consecuencia, convocamos a conformar un equipo de trabajo interdisciplinario para comprenderla mejor y saber cómo aprovecharla en bien del Estado y los ciudadanos.



2. Qué es la Cadena de Bloques

La primera mención de la tecnología de la *Cadena de Bloques* o Blockchain se hizo en el artículo *Bitcoin: un sistema de dinero en efectivo electrónico entre pares*, publicado en un foro en el año 2008 bajo el seudónimo de Satoshi Nakamoto, actualmente esta tecnología es mejor conocida como la plataforma base de la criptomoneda Bitcoin.

La Cadena de Bloques es como un libro de registros público y descentralizado diseñado para anotar las transacciones en un ambiente protegido.

Esta registración se almacena en una **red distribuida** de computadoras y no requiere de ninguna autoridad central, ni terceras partes que actúen como intermediarios certificantes.

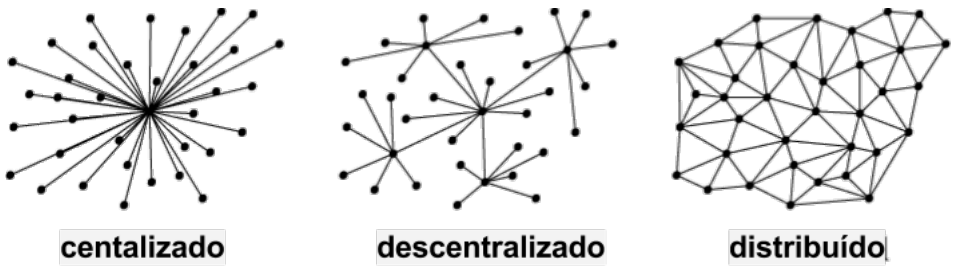


Figura 2.0.1: *Esquemas de organización de las redes*

En síntesis, es una base de datos que se usa para registrar transacciones dentro de un paquete de datos llamado **bloque**, los que son copiados en todas las computadoras que conforman la red.

Una de las características principales y una de las más relevantes, es la *inmutabilidad* de la cadena: no es posible modificar o borrar la información almacenada en los bloques.

Cada nuevo bloque, además de llevar la información horaria de su creación, contiene una referencia al bloque que lo antecede, creando así una relación lógica entre ellos: *la cadena*. De ahí deviene el nombre de esta tecnología: **La Cadena de Bloques**, o la Blockchain.

Esta secuencia creciente de bloques al ser públicos, conforman un sistema abierto que potencia la confianza en base a la multiplicidad, la transparencia y la solidez de la técnica de la construcción de la tecnología Blockchain.

Esta base de datos constituye un libro de acontecimientos digitales (transacciones, contratos, activos, identidades, o prácticamente cualquier cosa que pueda ser descrita en forma digital) que no requieren de la existencia de una institución intermediaria que identifique y certifique la información, sino que cada computadora miembro de la red (*los nodos*), registran y validan la información sin necesidad de que haya confianza entre ellos.

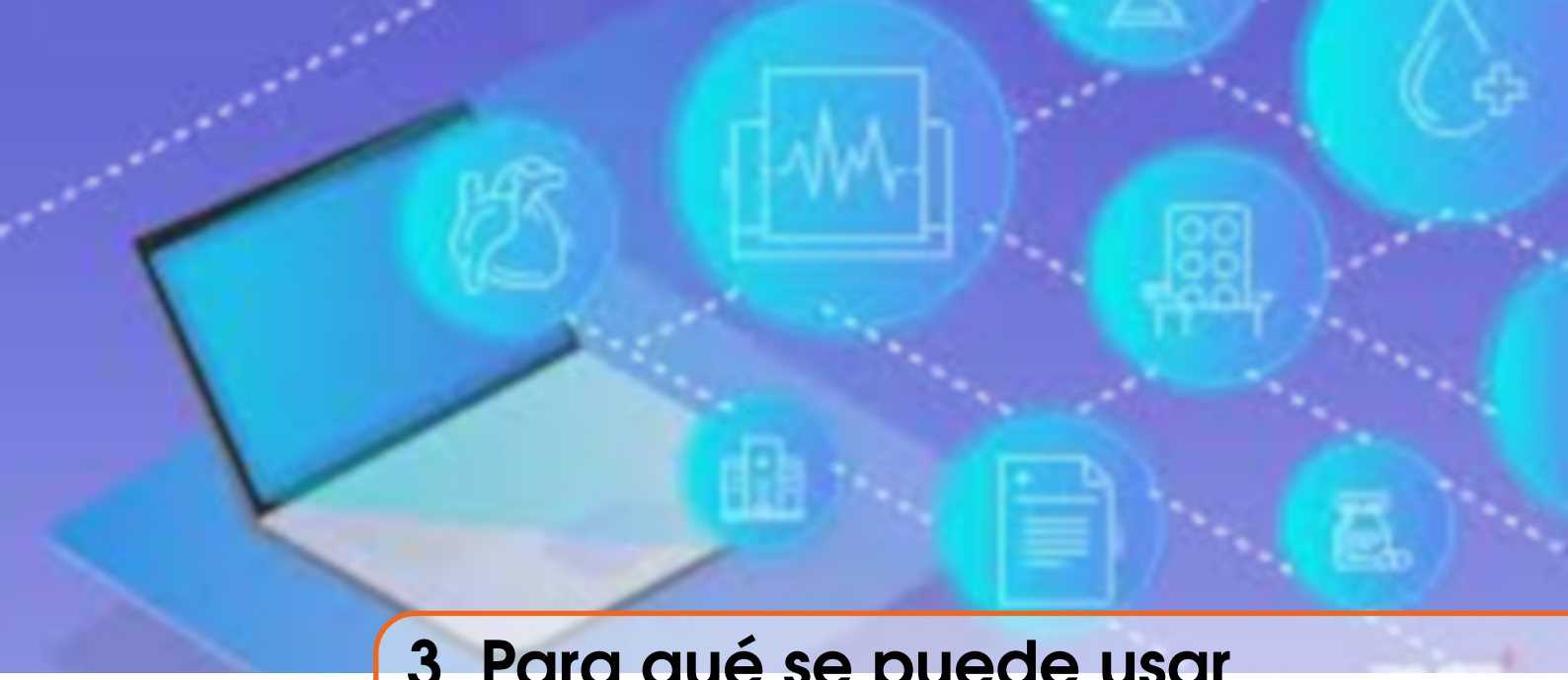
En esta red, cada nodo miembro mantiene una copia completa de la base de datos, y todos los miembros tienen que validar en forma colectiva cualquier actualización.

2.1 Características:

- Garantiza la identidad de las partes involucradas, ya que todas las transacciones se firman digitalmente.
- Certifica la fecha y hora de cada transacción.
- La información es inmutable e inalterable. No se puede modificar ni borrar.
- Toda la información auditable. Se agrega de forma pública y es visible por todos los usuarios.
- No tiene intermediarios. No hay una persona, empresa o institución que certifique la información guardada, ya que la cadena es segura por su propia naturaleza.
- Como los registros no se pueden borrar o modificar, solo agregar. Una cadena de bloques crece permanentemente.

II

Usos



3. Para qué se puede usar

Una de las cuestiones más críticas a considerar acerca de la Cadena de Bloques, es su potencial para transformar y reemplazar los procesos registrales.

Su potencial de uso es tan profundamente disruptivo, que requiere crear nuevos paradigmas hasta ahora totalmente inpensados en la administración pública.

En este sentido, sus posibilidades de uso se extiende a un inmenso abanico de aplicaciones, que implican a cualquier proceso registral que requiera una certificación o validación.

Lo transformador de esta nueva tecnología, es que **la validación y la seguridad la confiere la propia red** y no un organismo central con autoridad delegada para ello.

Sin ser una lista concluyente, las posibilidades de aplicación se extienden a:

- Registros de identidad de personas
- Registro de propiedad de inmuebles
- Títulos
- Diplomas
- Certificados
- Trazabilidad de productos
- Gestión de activos digitales
- Historias clínicas
- Protección de datos críticos

- Registro de nacimientos, defunciones y matrimonios
- Resultados de elecciones
- Guías de transporte
- Entrega de beneficios o subsidios
- Contrataciones

En síntesis, cualquier otra cosa que sea de interés para una organización y pasible de ser registrada digitalmente.

4. Cómo funciona

En un entorno tradicional, las transacciones electrónicas requieren intermediarios de confianza para dar seguridad a la transacción. Los intermediarios generan esta confianza y seguridad, llevando y preservando un registro centralizado de las operaciones electrónicas que permite controlar los datos de los intervinientes, y garantizar la autenticidad de cada transacción.

En la tecnología de la Cadena de Bloques, en lugar de tener la información centralizada en una sola computadora, y con unos pocos usuarios con privilegios para modificarla, los bloques están replicados en una serie de computadoras, bajo un modelo de red de pares que agregan datos sólo a partir del "consenso" (acuerdo) de las partes.

Esta tecnología es un software libre y gratuito que gestiona una base de datos distribuida, y que elimina la necesidad de terceras partes de confianza al hacer que una red de computadoras mantenga un libro de registros común que reside en la internet.

Este libro de registros es público y se distribuye en una red de computadoras (*nodos*), cada cual tiene una copia completa de la base de datos.

En ella, los detalles de cada transacción son registrados, marcados con la fecha y hora y luego son verificados por nodos denominados *selladores* de la red. Los registros se organizan en un paquete de datos denominado **bloque** y usualmente se publican en la base de datos a intervalos de diez minutos.

Los bloques están ordenados cronológicamente y se identifican por una clave, esta clave es un código alfanumérico conocido en la jerga como el *hash*, y están firmados digitalmente por la entidad que propone o valida el bloque.

Cada nuevo bloque contiene además de la información intrínseca de los registros, una referencia a los datos del bloque que lo antecede, de donde deviene en nombre de la *Cadena de Bloques*.

Esta técnica previene que pueda manipularse la información de los bloques, ya que están relacionados entre sí por su contenido. Por lo que cualquier alteración invalida el vínculo con los bloques adyacentes. Además, para alterar la cadena sería necesario modificar el 51 % de todos los bloques duplicados en toda la red en un período menor a los 10 minutos, lo cual es computacionalmente imposible.

5. Los contratos inteligentes

Una cuestión que merece un apartado diferente, tiene que ver con el concepto de los contratos inteligentes, conocidos también como *smart contracts*.

Se debe pensar a la Cadena de Bloques en un sentido amplio, en donde no sólo se registran transacciones, sino también porciones de programas de computadoras y reglas de ejecución de tareas.

Definimos como "contrato inteligente" a un algoritmo electrónico (o programa informático) que se ejecuta de forma autónoma y automática para dar cumplimiento a los términos de un acuerdo entre partes, y que se activará cuando se cumplan las condiciones estipuladas por las partes involucradas en el contrato en el momento de su firma.

Ya sean las personas como así también las máquinas pueden actuar como partes de un contrato inteligente, lo que habilita al funcionamiento de la Internet de las Cosas (IoT), donde no se necesita ninguna intervención humana en el proceso.

Estos no son contratos en el sentido extrictamente legal, sino que son programas que extienden la funcionalidad de la Cadena de Bloques, de ser un simple registro de asientos de transacciones a la implementación automática de los términos de los acuerdos.

El punto a tener en cuenta es que estos contratos no pueden ser modificados o anulados, y se ejecutarán indefectiblemente cuando se cumplan las condiciones preacordadas que lo activan.

6. Situación actual

El uso masivo de la Cadena de Bloques se inició con la criptomoneda Bitcoin, y gracias a su seguridad y versatilidad se extiende rápidamente a nuevos escenarios.

Los gobiernos innovadores del mundo ya se sumaron este nuevo paradigma tecnológico y comienzan a capitalizar sus beneficios.

6.1 En el mundo

6.1.1 Estonia

Una característica esencial del modelo de gobierno electrónico de Estonia es la identidad digital. Los estonios tienen un documento de identidad electrónico con el que pueden acceder a los servicios del Estado y viajar por la Unión Europea.

Estonia ofrece un sistema de ciudadanía electrónica (o “e-Residency”) a los extranjeros. Esta identidad digital permite a los extranjeros que pueden incluso vivir en otros países registrar empresas en Estonia, utilizar la banca digital y la firma electrónica. El funcionamiento de este sistema es posible gracias a la tecnología Blockchain, en la que se puede gestionar, registrar y almacenar incluso la información más sensible como los datos personales de forma segura y protegida. (DeMarinis, Uustalu, & Voss, 2017).

Usando su documento de identidad digital o su identidad móvil, desde el año 2005 pueden votar en las elecciones por internet y desde cualquier lugar del mundo.

Los estonios usan sus documentos de identidad electrónicos para revisar y editar en línea sus documentos fiscales, solicitar beneficios de la seguridad social y acceder a servicios bancarios y al transporte público. No necesitan tarjetas de bancos ni de transporte. Y pueden hacer lo mismo con una identidad digital que llevan en sus teléfonos móviles.

Estonia dispone de un registro inmobiliario electrónico que ha transformado el mercado del sector, reduciendo la duración del traspaso de propiedades de tres meses a poco más de una semana.

6.1.2 Ucrania

En Ucrania usan el sistema eAuction 3.0, un sistema de subasta electrónica para alquiler o venta de bienes de estado basado en la Blockchain para combatir la corrupción y disminuir la burocracia.

6.1.3 Suecia

Tiene un proyecto que permite concertar transacciones inmobiliarias de forma que todas las contrapartes – los bancos, los agentes, los compradores y vendedores – puedan tener la oportunidad de seguir el proceso de la implementación del acuerdo después de su finalización.

6.1.4 Inglaterra

Usa el registro distribuido para la gestión de subsidios. Como el control y el seguimiento de los subsidios concedidas es bastante complejo y muchas veces su uso indebido y el abuso es algo común, la tecnología Blockchain ofrece la mejor solución para este problema, ya que está accesible para todas las partes implicadas (Mougayar, 2016a).

6.1.5 Grecia

Posee un registro de propiedad de la tierra usando un prototipo de Blockchain, ya que el país no cuenta con un registro de este tipo y tan solo el 7 % del territorio está correctamente identificado.

6.1.6 Otros países

El registro catastral de tierras basado en la Blockchain ya está siendo implementado en Georgia, Grecia y Honduras. Algo similar están desarrollando en Ghana, África Occidental, donde la Blockchain va a permitir garantizar transparencia en las operaciones con inmuebles y sentar bases para la atracción de inversión extranjera.

6.2 En Argentina

6.2.1 Blockchain Federal Argentina

Se lanzó la iniciativa Blockchain Federal Argentina.

NIC Argentina, la Cámara Argentina de Internet - CABASE y la Asociación de Redes de Interconexión Universitaria (ARIU), colaboron en el desarrollo de una plataforma multiservicios de alcance federal basada en la tecnología Blockchain.

A través de esta iniciativa conjunta, en la que las partes representan al sector público, la academia y el sector privado, se conformó la infraestructura sobre la que corre la primera plataforma nacional de uso público basada en Blockchain, una innovadora tecnología de validación de transacciones.

https://nic.ar/es/enterate/novedades/se-lanzo-bfa

6.2.2 Universidad Provincial del Sudoeste (UPSO)

Para que no haya más títulos apócrifos, cobra fuerza Blockchain y una universidad argentina ya lo aplica.

La tecnología detrás del bitcoin garantiza la veracidad de los certificados y ofrece ventajas al graduado.

Para dar comienzo a la prueba, se aliaron con la empresa de Singletally.com, que les recomendó utilizar la aplicación de un protocolo creado por el Instituto Tecnológico de Massachusetts (MIT). El sistema se llama *blockcerts* y hace que todos los títulos que se emiten a nivel mundial tengan el mismo protocolo. De ese modo, se homogeneiza la emisión de certificados.

https://www.infobae.com/educacion/2019/01/05/para-que-no-haya-mas-titulos-truchos-cobra-fuerza-blockchain-y-una-universidad-argentina-ya-lo-aplica/

6.2.3 El Municipio de Bahía Blanca

Se aplicó al proceso de subsidios de cultura de la municipalidad por ser un proceso sencillo, con una cantidad razonable de actores y en el que se manejan fondos públicos.

Pensemos en la utilidad de esta innovación para licitaciones o compras: que la oferta o el momento de presentación de la misma, no pueda ser alterada por terceros o involucrados. La finalidad de la experiencia era demostrar que Blockchain puede ser utilizado como un notariado digital de información pública, dando seguridad a procesos de gobierno que impliquen asignación de subsidios, compras o licitaciones.

6.2.4 dtecdeal

Blockchain tendrá en Argentina la primera plataforma para contratos

Un estudio jurídico de La Plata ofrecerá este servicio, el primero a nivel global, para pactar contratos nacionales e internacionales con el máximo margen de seguridad.

https://www.infobae.com/economia/finanzas-y-negocios/2018/11/28/Blockchain-tendra-en-argentina-la-primera-plataforma-para-contratos/

6.2.5 Signatura

Signatura es una empresa dedicada al desarrollo de soluciones de avanzada para procesos de firma y certificación digital. Es miembro de OpenTimestamps, un sistema descentralizado de sellado de tiempo que utiliza la blockchain de Bitcoin para probar la existencia de documentos. Interactúa normalmente con servidores de calendario para agrupar peticiones y registrar atestaciones.

https://signatura.co/es/

Buenos Aires se prepara para ser la capital Blockchain de América Latina.

https://www.cronista.com/finanzasmercados/Buenos-Aires-se-prepara-para-ser-la-capital-Blockchain-de-America-Latina-20181114-0099.html

III

Conclusiones

7. Conclusiones

La Cadena de Bloques tiene el potencial de causar una disrupción total en los modelos de gestión tradicionales y en el corto plazo hacer obsoletos ciertos paradigmas de la cultura organizacional.

Por este motivo los líderes mundiales de la industria y los gobiernos innovadores están invirtiendo en la investigación, el desarrollo y la prueba de aplicaciones basadas en la tecnología de la Cadena de Bloques.

Si se incluyeran los documentos oficiales (DNI, partida de nacimiento, certificado de matrimonio, certificado de defunción, carnet de conducir, tarjeta sanitaria, títulos de propiedad, condición fiscal y laboral, expedientes académicos, etc.) que hoy existen en diferentes bases de datos dispersas, en una cadena de bloques integrada, las redes podrían ofrecer servicios integrados sin necesidad de pasar por un procesamiento central. Este modelo no sólo protege la privacidad, sino también la aumenta, porque permite comprobar la veracidad de la información y saber quién accede a ella o la modifica (una especie de auditoría permanente).

El despliegue de esta tecnología debe ser desarrollado en el marco de un *plan estratégico* que entienda las necesidades del proyecto, identifique el grado de transparencia y descentralización, determine los miembros que actuarán como nodos y establezca la estructura de bloques adecuada, definiendo cómo van a ser las transacciones y los contratos inteligentes que se van a ejecutar.

TODO ES BLOCKCHAIN. O AL MENOS, TODO LO SERÁ.

IV

Referencias

Glosario

Bitcoin Bitcoin es un protocolo y red entre pares (P2P) que se utiliza como criptomoneda, sistema de pago y mercancía. 9

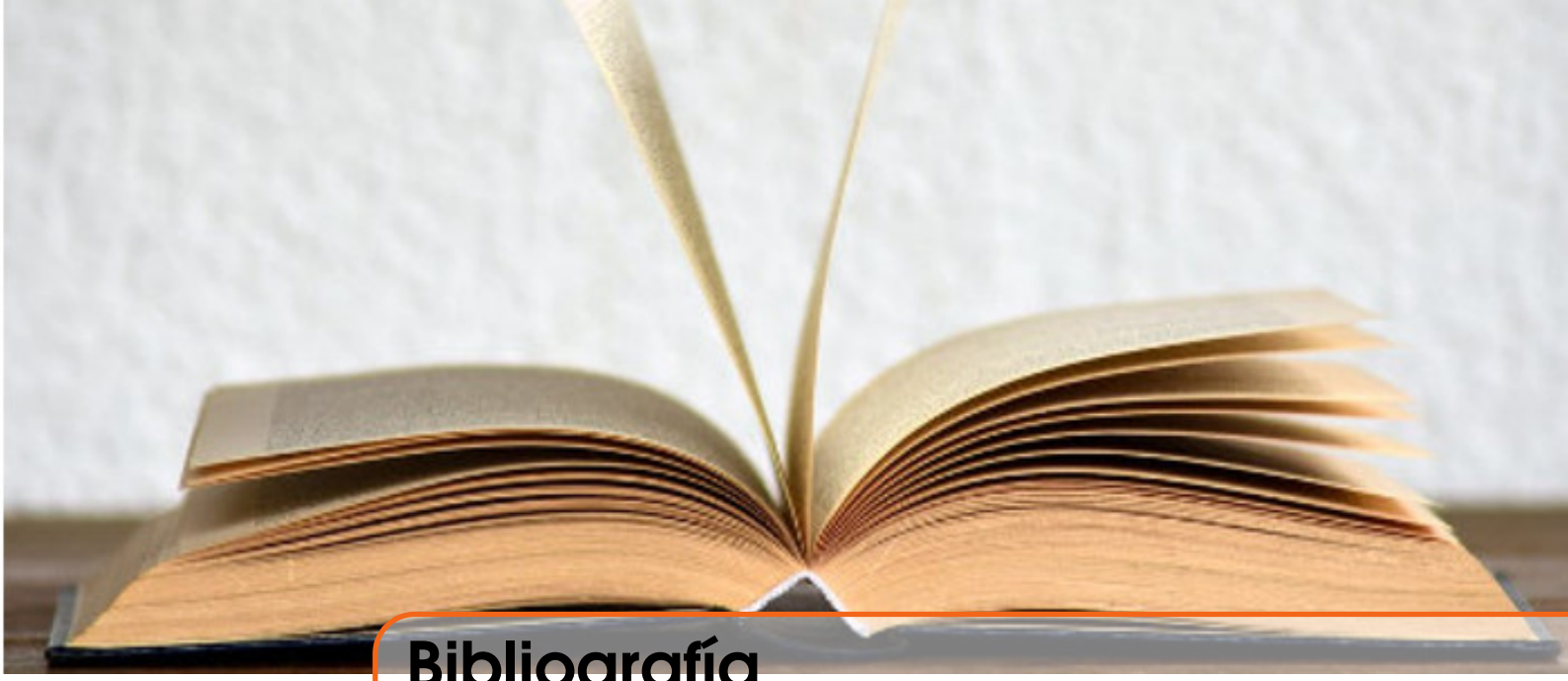
Blockchain Es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se les añade metadatos relativos a otro bloque de la cadena anterior en una línea temporal, de manera que gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores. Esta propiedad permite su aplicación en entorno distribuido de manera que la estructura de datos blockchain puede ejercer de base de datos pública no relacional que contenga un histórico irrefutable de información. 9

criptomoneda Una criptomoneda, criptodivisa o criptoactivo es un medio digital de intercambio que utiliza criptografía fuerte para asegurar las transacciones financieras, controlar la creación de unidades adicionales y verificar la transferencia de activos. Las criptomonedas son un tipo de divisa alternativa y de moneda digital. Las criptomonedas tienen un control descentralizado, en contraposición a las monedas centralizadas y a los bancos centrales. 9

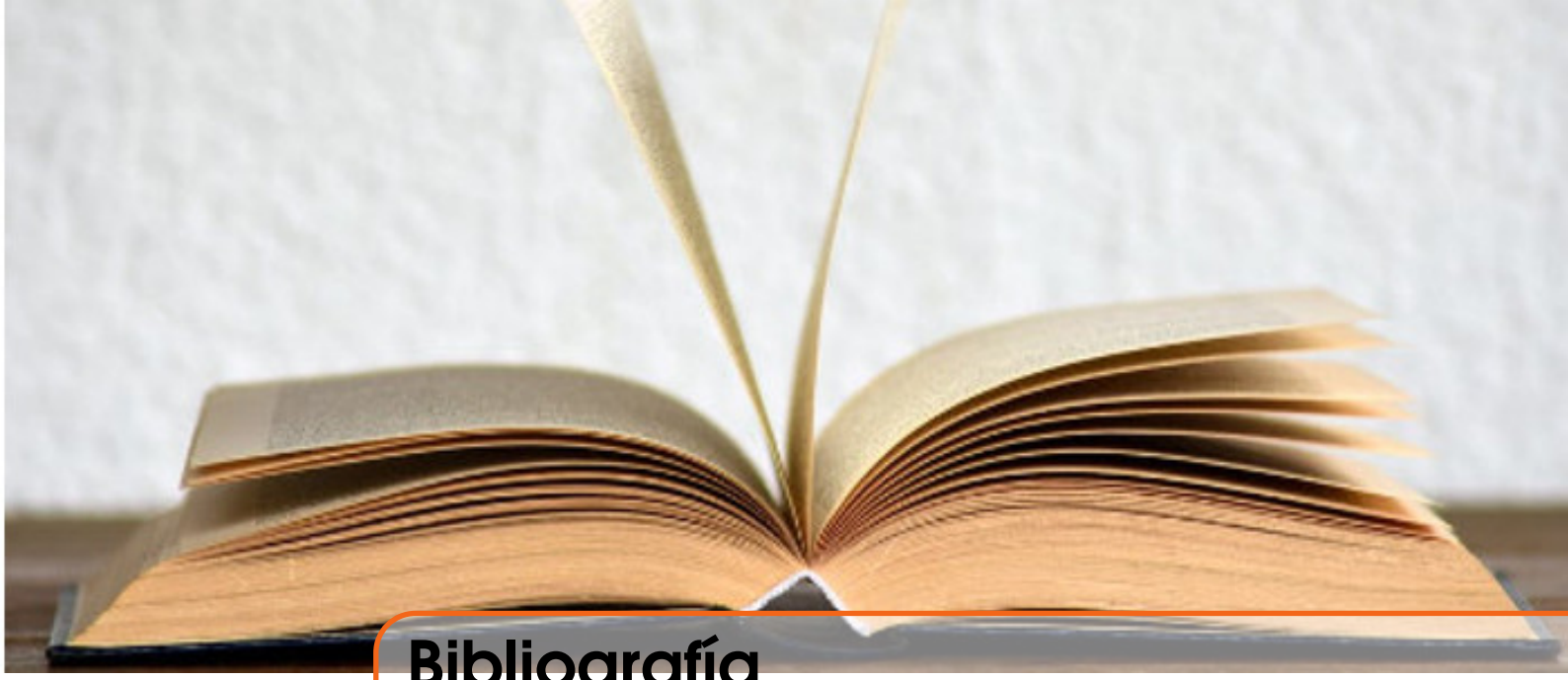
hash Una función criptográfica "hash" es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. 15

Internet de las Cosas Es un concepto que se refiere a una interconexión digital de objetos cotidianos con internet. Es, en definitiva, la conexión de internet con más objetos que con personas. 17

software libre El software libre es todo programa informático cuyo código fuente puede ser estudiado, modificado, y utilizado libremente con cualquier fin y redistribuido sin o con cambios y/o mejoras. 15



Bibliografía



Bibliografía

[1] Satoshi Nakamoto (2008), Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer, www.bitcoin.org.

[2] Dan Tapscott & Alan Tapscott (2017), La Revolución Blockchain. Descubre cómo esta nueva tecnología transformará la economía global, Ed. Duesto.

[3] Anastasiia Zemlianskaia (2017), Tecnología Blockchain como Palanca de Cambio en el Sector Financiero y Bancario.

[4] BBVA Innovation Center (2016), Tecnología Blockchain.

[5] Semana Económica, (2017), Edición 1084, Blockchain: mirando más allá del Bitcoin.

[6] Deloitte Insights (2017), Tech Trends 2017, Blockchain: Economía de confianza.

[7] Marcos Allende López (2018), Blockchain. Cómo desarrollar confianza en entornos complejos para generar valor de impacto social, ITE/IPS TechLab - BID.

[8] Lucas Jolías (2017), Blockchain, transparencia y el futuro del Gobierno Abierto, Jornadas Académicas En Gobierno Abierto.

[9] Jesús Cepeda, Agustina De Luca, Lucas Jolías, Denise Zelaya (2017), Blockchain y Transparencia: La Experiencia en la Ciudad de Bahía Blanca, Fellowship OEA en Gobierno Abierto para las Américas.

[10] Carlos Dolader Retamal, Joan Bel Roig, Jose Luís Muñoz Tapia, (2017) La Blockchain: Fundamentos, Aplicaciones y Relación con Otras Tecnologías Disruptivas. Economía industrial, ISSN 0422-2784, Nº 405.