ARTÍCULOS

BOLETÍN CIENTÍFICO TECNOLÓGICO

ACADEMIA POLITÉCNICA MILITAR

BLOCKCHAIN Y SU APLICACIÓN EN CIBERDEFENSA

SG2. ROBERTO SOTO YANCA

BLOCKCHAIN Y SU APLICACIÓN EN CIBERDEFENSA

SG2. Roberto Soto Yanca[1]

Resumen: *blockchain forma parte y sustenta el mecanismo de funcionamiento detrás de las llamadas "criptomonedas", siendo estas últimas una de las muchas aplicaciones de esta tecnología. El funcionamiento y la particularidad de la blockchain radica en el concepto de descentralización y en la distribución entre sus nodos (computadores participantes que entran voluntariamente a cadenas de bloques abiertas o a las cerradas, por invitación). Otra característica destacable es su sistema de cifrado o codificación, dada la inmutabilidad de los registros y su trazabilidad o seguimiento. En el sector de la defensa, esta tecnología podría ser vista como una solución al control de cadenas de suministros, amenazas a la ciberseguridad, comunicaciones e, incluso, en obtener autorización para la activación de un sistema de armas. En el presente artículo serán analizados diversos sectores de la industria a nivel mundial que están utilizando esta tecnología con la intención de presentar de manera resumida el uso de blockchain.*

Palabras clave: *blockchain, descentralización, nodo, cifrado, ciberdefensa, peer to peer.*

Abstract: *blockchain is part of and the sustenance of the "cryptocurrencies"operation mechanism, one of the many applications of this technology. The operation and the particularity of the blockchain lies in the concept of decentralization and in the distribution between the nodes (participating computers that enter voluntalary to the open chains or to the closed ones through and invitation). Another outstanding feature is its encryption or coding system,due to the immutability of the records and their traceability or monitoring. In the defense sector, this technology could be seen as a solution for the supply chains control, the threats against cybersecurity, communications, and even to obtain authorization to activate the weapons system. In this article,*

1 Mecánico de Equipos de Telecomunicaciones. Técnico Nivel Superior en Ciberdefensa (ACAPOMIL). Profesor Militar de Escuela (Seguridad Militar).

will be analyzed several worldwide sectors of the industry that are using this technology with the intention of presenting a summarized way the blockchain use.
Keywords: *blockchain, decentralization, node, encryption, cyberdefense, peer to peer.*

1. INTRODUCCIÓN

Es necesario aclarar previamente que lo innovador de esta tecnología y su incipiente uso en la industria a nivel mundial, implica que la literatura disponible sobre *blockchain* y temas relacionados sea escasa, por lo que se debió acudir a bibliografía digital.

Cuando en mayo de 2008 se produjo la erupción del volcán Chaitén, el fenómeno terminó por arrasar con la mitad de la ciudad, producto del daño colateral, principalmente ocasionado por un aluvión y posterior desbordamiento de los cursos de agua cercanos. Al día siguiente, el gobierno debió realizar una costosa y peligrosa operación para recuperar la bóveda del Conservador de Bienes Raíces del pueblo, porque, de no ser posible rescatarla, se perderían todos los títulos de dominio de la zona.

Más recientemente, en enero de 2019, se registró un incendio intencional que destruyó el Juzgado de Letras de Rapa Nui, además de una notaría y otros edificios, en el marco de una manifestación por la muerte de un isleño. Las llamas fueron provocadas por un grupo de personas que intentaron atacar al agresor durante la audiencia de formalización que se realizaba en el lugar. En los dos edificios, se encontraba documentación e información importante, la que se perdió producto de las llamas.

En ambos casos, resulta relevante la opinión de Julio Pertuzé,2 Jefe de la División de Economía del Futuro del Ministerio de Economía, en una entrevista a Emol.com, donde a raíz de lo ocurrido en Chaitén, indica que: “toda esa información, que era crítica y valiosa, estaba centralizada en un solo lugar. Era vulnerable […] algo que con la tecnología *blockchain*, jamás habría ocurrido” (Pertuzé, 2018).

---

2 Julio Pertuzé es Ingeniero Civil de Industrias de la Pontificia Universidad Católica de Chile (PUC), con Ph.D. en Ingeniería de Sistemas y M.Sc. en Tecnología y Políticas Públicas del Massachusetts Institute of Technology. Desde el 2013 es profesor del Departamento de Ingeniería Industrial de la PUC y Codirector del Magíster de Innovación UC. Sus principales áreas de investigación son la Gestión Estratégica y las Políticas Públicas de Ciencia, Tecnología y Educación Superior.

2. *BLOCKCHAIN*

Blockchain, traducido como "cadena de bloques", es considerada la revolución industrial de Internet, o el siguiente paso a ella, ya que se pasa de la etapa de una 'Internet de la información' a una de 'Internet del *valor'* (Preukschat, 2017),[3] dado que como actualmente en Internet es posible distribuir de forma libre información sin intermediarios, con *blockchain* se puede hacer algo similar, pero con activos. También conocido como la "Internet de la confianza", *blockchain* permite transferir activos digitalizados entre los usuarios, a diferencia de la Internet clásica que solo permite enviar información o copias de activos. La propia red actúa como un "ministro de fe", manteniendo un acuerdo sobre la existencia, estado y la evolución de los elementos compartidos. O desde un punto de vista técnico, este sistema, basado en la confianza y el consenso, está construido a partir de una red de computadores que gestionan una gigantesca base de datos.

Es una tecnología perteneciente al ámbito de las DLT (Distributed Ledger Technologies) traducido como "Tecnologías de Registro Distribuido". Esto, debido a que la información que se encuentra en *blockchain* se encuentra disponible públicamente. Es descentralizada, lo que significa que no se encuentra en un solo servidor, de tal manera que todas las transacciones son visibles para todo el mundo.

Para entender su funcionamiento, es necesario conocer, al menos, los elementos básicos que la conforman. El primero corresponde a los nodos, que son los equipos informáticos de la red que sostienen la cadena y que, al mismo tiempo, almacenan los registros tal como un libro mayor de contabilidad, por lo tanto, conforman su infraestructura.

El segundo elemento es la red, conformada por todos los nodos, los que son iguales entre sí. Esto se traduce en una red entre pares o P2P (peer to peer).

Un tercer elemento se refiere al protocolo, con el cual se crea el procedimiento de registro. Con este se alcanza un acuerdo entre los nodos sobre la versión válida de dicho registro. Esto asegura que exista solo una versión inmodificable y auditable de los datos almacenados y de los movimientos o transacciones realizadas.

---

3 Alex Preukschat es el autor de la primera novela gráfica de Bitcoin del mundo (BitcoinComic.org), el best seller de *Blockchain*, Libro*Blockchain*.com, coordinador de *Blockchain* España (*Blockchain*Espana.com), Alianza *Blockchain* Iberoamerica (Alianza*Blockchain*.org) y de la Identidad Autónoma y Comunidad para la identidad digital descentralizada SSIMeetup.org. Es creador de juegos móviles de criptomoneda con MoneyFunGames.com.

Otro elemento son las cadenas de bloques, que se asemeja a un libro de contabilidad digital donde se anotan todas las transacciones que suceden en la red, agrupadas en bloques que continuamente son enlazados linealmente entre sí, donde el primer bloque se enlaza con el segundo, el segundo con el tercero y así sucesivamente (de allí el nombre de "cadena de bloques").

Las *wallets* o "billeteras digitales", por su parte, corresponden a las aplicaciones o interfaces en las que los usuarios hacen sus transacciones y gestionan su identidad digital (ID). Son operables mediante el uso de una clave privada y una clave pública.

Finalmente, existe un subgrupo de los nodos llamados "mineros", especialmente en las redes de criptomonedas y que corresponden a computadores que ponen a su disposición su capacidad de procesamiento, para realizar el trabajo de validación que autoriza que se añadan nuevos bloques a la cadena. Para esto, deben resolver un problema matemático, siguiendo un protocolo de consenso criptográfico de enorme y deliberada complejidad (Cabrera, 2018).[4]

3. FUNCIONAMIENTO DE *BLOCKCHAIN*

Como muestra la Figura Nº 1, el funcionamiento de una transacción común de *blockchain* comienza de la siguiente forma:

3.1 Envío

El usuario "A" realiza el envío de un activo digital desde una *wallet* o billetera digital hacia otro usuario identificado como "B". Lo que ocurre en este punto es en realidad el envío de una versión *hash* (resumen cifrado o criptográfico) de lo que se conoce como Clave Pública. La clave pública de "B" es conocida por todos en la red y, en este caso, es utilizada por "A" para cifrar el mensaje.

3.2 Validación

La transacción es examinada y autorizada por distintos nodos y, posteriormente, agrupada con otras transacciones.

---

4 Fabiola Cabrera V. es Magíster en Asuntos Públicos del Instituto de Ciencias Políticas de París y Magíster en Gestión e Ingeniero Comercial, por la Pontificia Universidad Católica de Valparaíso. Actualmente dicta el curso de Globalización e Innovación para Ingeniería Industrial PUCV.

3.3 Minería

Las transacciones son tomadas por los mineros como un trabajo para resolver a cambio de una retribución (criptomonedas). Ellos eligen un grupo de transacciones, que puede ser diferente para cada agrupación de mineros y compiten por conseguir un "valor" (nonce), el que obtienen resolviendo un problema matemático, que autoriza al minero que lo resolvió a proponer su bloque con las transacciones que contiene y, luego, ser agregado a la cadena de bloques. El bloque contiene, además, la identificación y *hash* (resumen criptográfico) del bloque anterior, estableciéndose la linealidad de la cadena.

3.4 Distribución

Todas las cadenas de bloques se guardan en los computadores que forman parte de la red, por lo que no existe una base de datos única que pueda ser atacada. Un potencial atacante debería tener el control de, a lo menos, un 51% de la red para intentar conseguir su objetivo. A diferencia de las bases de datos centralizadas, *blockchain* crea una base de datos descentralizada, distribuida, compartida y replicada.

3.5 Recepción

El usuario "B" recibe el mensaje proveniente desde "A". Lo que ocurre en este punto es que "B" toma el *hash* recibido y utiliza su clave privada (la cual solo él conoce) para descifrar el mensaje.

Figura Nº 1: "Funcionamiento de *Blockchain*".

Fuente: BBVA, 2018.

4. SISTEMA DE ENCRIPTACIÓN

Gracias a la criptografía[5] y al mecanismo detrás de *blockchain*, la adulteración de los datos se hace casi imposible. De esta manera, se asocia a *blockchain* con la confiabilidad, disponibilidad e integridad de la información.

Por ende, el sistema de encriptación es fundamental en esta tecnología. En 1976, Whitfield Diffie y Martin Hellman crearon el algoritmo del protocolo criptográfico que lleva sus nombres. Es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro y de manera anónima. El sistema se basa en la idea de que dos interlocutores, pueden crear en conjunto una clave compartida sin que un extraño, que esté interceptando las comunicaciones, pueda llegar a obtenerla. Para ello propusieron dividir las claves encriptadas en dos claves: una pública y una privada (criptografía asimétrica).[6] Con la clave pública se puede cifrar un mensaje, pero para descifrarlo es necesaria la clave privada. Estas claves (llamadas Keys en inglés), están formadas por grandes combinaciones de letras y números.

Para lo anterior, se elige un número público (clave pública) y un número secreto (clave privada). Usando una fórmula matemática, que incluye la exponenciación, cada interlocutor hace una serie de operaciones utilizando la clave pública y la clave privada.

La clave privada se usa para obtener la clave pública. Cada usuario tiene su clave privada, pero esta nunca debe ser compartida con otras personas. La clave privada es la más larga de las dos y se usa para generar una firma para cada mensaje que envía un usuario. Esta firma es usada para confirmar que la transacción ha sido realizada por ese usuario (principio de no repudio)[7] y, además, prevenir que la transacción sea modificada por cualquier persona una vez que ya ha sido realizada. A continuación, ambas partes intercambian sus respectivas claves públicas. La clave pública se usa junto con la información en la red y una suma de comprobación, para transformarla en la dirección *hash* que otras personas pueden ver.

---

5 Criptografía es la ciencia y arte de escribir mensajes en forma cifrada o en código. Es parte de un campo de estudios que trata las comunicaciones secretas. A partir de la evolución de las computadoras, la criptografía fue ampliamente divulgada, empleada y modificada y se constituyó luego con algoritmos matemáticos.

6 El sistema matemático que soporta a este principio de criptografía solo puede ir en una dirección; en consecuencia, aplicar cualquier intento por descifrar una clave con la otra es prácticamente imposible, es decir, que la clave pública (Public Key) existe porque existe la llave privada (Private Key), no de forma inversa.

7 El no repudio es un servicio de seguridad que permite probar la ejecución de un proceso (transacción, comunicaciones, etc.). El no repudio en el origen: el emisor no puede negar que envió el mensaje, porque el destinatario tiene pruebas del envío; el no repudio en el destino: el receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción.

La suma de comprobación o verificación es una parte de la información que sirve para detectar cambios accidentales en la secuencia de datos y, así, proteger la integridad de los mismos. En el caso de la clave pública, la suma de comprobación es necesaria para verificar que no haya sido alterada y, de esta forma, evitar problemas de recepción de la misma. El receptor termina recibiendo el mensaje que otra persona le envía a través de esta dirección.

Para entender de mejor manera su funcionamiento, la Figura Nº 2 muestra una analogía de ejemplo del intercambio de un mensaje utilizando criptografía asimétrica, donde el usuario "A" quiere enviar un mensaje secreto que solo pueda ver el usuario "B".

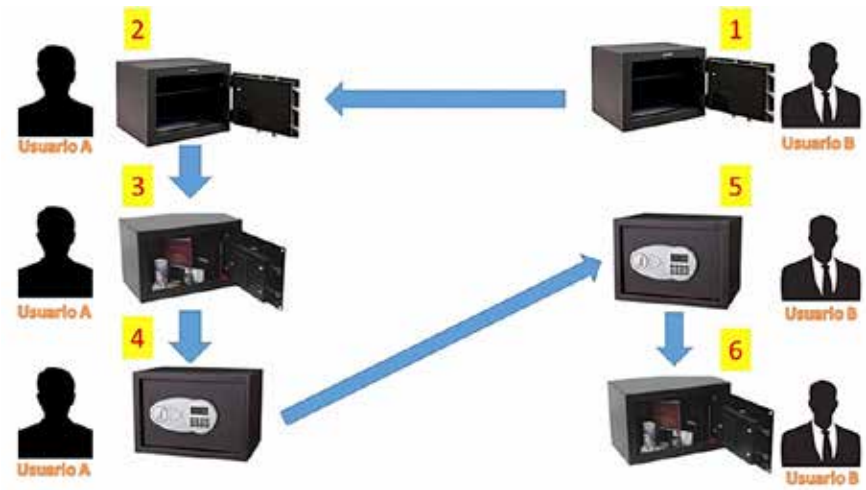

Figura Nº 2: "Criptografía asimétrica".

Fuente: elaboración propia.

En este ejemplo, la caja con la cerradura abierta es la "clave pública" del usuario "B", y la clave que abre la cerradura es su "clave privada". En primer lugar, debemos imaginar que el usuario "B" envía al usuario "A" una caja fuerte abierta, pero que cuenta con una cerradura electrónica. La cerradura se bloqueará una vez que el usuario "A" cierre la puerta de la caja y solo podrá abrirse con una clave, que únicamente el usuario "B" conoce. Luego de que el usuario "A" recibe la caja abierta, pone en ella lo que necesita enviar, cierra la caja fuerte usando su cerradura (ahora el usuario "A" ya no podrá abrir la caja) y, finalmente, envía la caja al usuario "B", quien la abre, utilizando su clave privada.

En este punto es válido preguntarse: si alguien tiene una clave pública, ¿debe existir un método inverso para obtener la clave privada? En teoría, revertir esta función es un sextillón (10^{36}) de veces más difícil que la exponenciación usada para transformar los números. Esto implica que si quisiéramos hacer el mecanismo inverso, se requerirá del computador más poderoso del mundo, el cual, en teoría, tardaría más de 4 seguido de 31 ceros años

(4^{31}), para completar el cálculo. El algoritmo hace fácil generar la clave pública a partir de la privada, pero es muy difícil o casi imposible en la actualidad hacer la operación inversa.

5. INTERNET DE LAS COSAS (IOT)

Se hace necesario mencionar Internet de las cosas para hablar de futuras aplicaciones de *blockchain*. La Internet de las cosas (IoT, por sus siglas en inglés) es una red de objetos físicos (vehículos, máquinas, electrodomésticos, entre muchos otros) que utiliza sensores e interfaces de programación de aplicaciones (API) para conectarse e intercambiar datos por Internet (Sap, 2019).[8] Todos estos dispositivos se interrelacionan y forman un sistema, que incluye, incluso, animales y personas, que se individualizan y se identifican dentro de la red, siendo capaces de transferir datos en ella, sin requerir de la intervención entre humanos o entre humanos y computadores. En la actualidad, desde un teléfono inteligente o una tablet, es posible configurar y administrar desde un solo lugar y, de manera eficiente, todos los equipos electrónicos y dispositivos que tengan conectividad en un hogar, como luces, cerraduras, alarmas, refrigeradores, aspiradoras, televisores e, incluso, lavadoras. Antonella Solari, gerente de productos móviles de Samsung Chile (Samsung, 2018),[9] señala que: "con este tipo de innovaciones, podemos responder a las diversas necesidades de los usuarios como son el ahorro de tiempo, eficiencia de recursos y comodidad para administrar los diversos dispositivos al interior del hogar y, de esta forma, contribuir con la calidad de vida de las personas". Los usuarios configuran los dispositivos para que funcionen de forma automática según sus necesidades y estos últimos, a su vez, entregan información a los propietarios de su estado. Con equipos que conocen todo lo relacionado sobre sus funciones, utilizando datos que recopilaron automáticamente, pueden rastrear y contar todo, reducir los desechos, las pérdidas y los costos. Los humanos sabríamos cuándo necesitamos reemplazar, reparar o eliminar cosas.

6. APLICACIÓN DE *BLOCKCHAIN*

Existen *blockchain* públicas y privadas y se diferencian porque las públicas pueden ser integradas por cualquier persona o entidad libremente (cumpliendo con requisitos

8 Fundada en 1972, SAP es el líder del mercado en *software* de aplicaciones empresariales, que ayuda a las empresas de todos los tamaños y en todas las industrias a funcionar de la mejor manera: el 77% de los ingresos de transacciones del mundo toca un sistema SAP. El aprendizaje automático, Internet de las cosas (IoT) y tecnologías avanzadas de análisis ayudan a convertir los negocios de los clientes en empresas inteligentes.

9 Samsung es el mayor grupo empresarial surcoreano. En 2012 se convirtió en el mayor fabricante mundial de telefonía móvil al superar a Nokia, que lideraba el mercado desde 1998. Fue reconocida por Booz & Co. y Boston Consulting Group, en 2013, como la segunda empresa más innovadora del mundo, por detrás de Volkswagen, luego de aumentar un 15% las partidas de I+D+i.

mínimos para su funcionamiento), mientras que en las privadas o cerradas, los nodos participantes deben ser invitados a integrar la red, como puede ser un grupo empresarial, una organización de gobierno, o en el caso de la defensa, una red de unidades militares. En las *blockchain* públicas, existe un sistema descentralizado en donde la información está distribuida por igual en todos los nodos, mientras que en las privadas, podría existir una jerarquía (Cabrera, 2018). A diferencia de las tradicionales bases de datos centralizadas que se alojan en un organismo central o en sus servidores, con el uso de *blockchain* es posible crear una base de datos distribuida, descentralizada, compartida y replicada. Los datos o transacciones registradas deben ser inalterables, controlables, poseer protección criptográfica y contar con un sistema de verificación de su autenticidad, tarea realizada por los nodos validadores. De esta forma, es posible el registro de las distintas transacciones en una base de datos descentralizada, facilitando el intercambio de información entre las partes de manera eficiente, abierta y verificable. Todos pueden ver lo que existe en la cadena y cualquier intento de alteración es descubierto de inmediato.

Blockchain aparece respaldado por su sistema criptográfico de clave pública y privada, como una solución a las graves vulnerabilidades que enfrenta Internet, con la posibilidad de aplicarla militarmente en temas de ciberseguridad, autorización y/o transmisión de órdenes, o algún tipo de mensaje en el caso de las comunicaciones, de manera indescifrable por terceros. Los *Smart Contracts* (contratos inteligentes) son un ejemplo de su aplicación: se trata de un protocolo informático o líneas de código programadas, que incorpora instrucciones para ejecutar un contrato de manera automática, siempre y cuando se cumplan las cláusulas preestablecidas. En el caso de un sistema de armas o de algún sistema de defensa, un *Smart Contract* podría activar un protocolo determinado de forma automática al cumplirse los escenarios previamente programados, sin la necesidad de la intervención humana, ya que no es necesario acudir a agentes externos para ejecutar la condición prevista, ni tampoco necesitan la intervención de personas para comprobar y ejecutar su cumplimiento.

La combinación del uso de la tecnología *blockchain*, la Internet de las cosas (IoT) e instrumentos como los *Smart Contracts*, permiten visualizar muchas posibilidades en distintos ámbitos de aplicación militar y que, actualmente, se están llevando a cabo por diferentes organismos en el mundo como a continuación se detallan.

6.1 Sistemas de seguridad y autorizaciones automáticas

En combinación con IoT, se pueden generar *Smart Contracts* que funcionen como autorizaciones inteligentes o una especie de cerradura digital, que solo les otorgue acceso o disponibilidad a los usuarios que sean autorizados.

Porsche, en colaboración con la empresa XAIN,10 se encuentra probando aplicaciones *blockchain* directamente en sus vehículos, con resultados satisfactorios. Las aplicaciones incluyen bloquear y desbloquear el vehículo para su uso, autorizaciones de acceso temporal al vehículo, así como la implementación de los denominados contratos inteligentes. Según Oliver Döring, de Porsche,11 las operaciones basadas en *blockchain*, "son seguras y pueden procesarse mucho más rápido que cualquier otra solución anterior" y podrían abrir un novedoso camino hacia el desarrollo de la conducción autónoma. En palabras de Döring (2018):

> Podemos usar *blockchain* para transferir datos de forma más rápida y segura, lo que brinda a nuestros clientes más tranquilidad en el futuro, ya sea que estén cargando su vehículo, estacionando o necesiten dar acceso temporal al coche a un tercero, como puede ser un agente de entrega de paquetes. Tomando 1,6 segundos, el proceso de abrir y cerrar el automóvil a través de una aplicación es hasta seis veces más rápido que antes. Además, tiene lugar un encriptado criptográfico eficiente. Este proceso asegura que todas las actividades estén documentadas en el *blockchain* de una manera que evite que se modifiquen y se puedan ver mediante una aplicación. Por ejemplo, las autorizaciones de acceso pueden distribuirse de forma digital y segura y pueden ser supervisadas por el propietario del vehículo en cualquier momento.

6.1.1 *Blockchain* en aplicaciones militares

En aplicaciones militares, el uso de *blockchain* aseguraría la protección de todas las comunicaciones entre los involucrados, permitiendo, además, un acuerdo colectivo utilizando los contratos inteligentes, en el que se puede conceder, por ejemplo, la autorización para el uso de un vehículo o el acceso a alguna instalación, activando los permisos cuando se cumplen condiciones previamente definidas.

La cadena de bloques es una base de datos que se encuentra compartida y distribuida y actúa como un libro de registros inalterable. Cada vez que se registra una

---

10 XAIN comenzó como un proyecto de investigación de la Universidad de Oxford en 2014 y se incorporó a Berlín en febrero de 2017. Con oficinas en Berlín, Stuttgart y Oxford, ofrece servicios en Europa, el Reino Unido y en todo el mundo. Dados los antecedentes de los fundadores y la experiencia en la industria automotriz, XAIN mantiene un fuerte enfoque de investigación y se especializa en brindar soluciones de infraestructura digital para el sector de la movilidad (https://xain.io).

11 Porsche AG es un fabricante de automóviles alemán especializado en automóviles deportivos lujosos, de alta gama, SUV y sedanes. Es propiedad del Grupo Volkswagen, que, a su vez, es propiedad mayoritaria de Porsche Automovil Holding SE.

autorización, esta se marca con un código único que la posiciona en el lugar secuencial que le corresponde.

En aplicación militar, lo anterior significa que las autoridades involucradas pueden usar sensores y dispositivos para recopilar datos sobre los vehículos, sistemas de armas o instalaciones. Esta información es ingresada a la *blockchain* y, en el caso concreto de un vehículo, puede incluir lecturas como niveles de combustible, estado operativo, así como su ubicación, para mantener un control si este se trasladara a plantas de revisión, talleres u otros puntos de la cadena de mantenimiento.

Las autoridades pueden determinar, mediante estos sensores, cuándo un vehículo está listo para ser empleado, lo que, a su vez, puede ser comunicado a los mandos directos y/o a otros involucrados. Además, al compartir distintos datos, un vehículo puede darle, a los que tomen decisiones, una noción sobre su disponibilidad, lo que ayudará a toda la cadena de mando a organizarse mejor y no tener que buscar soluciones de último minuto.

6.2 Gestión de identidades

Es uno de los ámbitos con mayor futuro en la actualidad, ya que las ID de *blockchain* en el futuro podrían reemplazar a las actuales credenciales (usuario y contraseña) y a la firma digital. Cada usuario guardará los datos que desee dentro de su identidad digital y dará acceso a quien estime conveniente de datos específicos para un fin determinado. Un ejemplo de esto, sería la posibilidad de garantizar los sistemas de voto electrónico, ya que cada usuario solo podrá votar una vez, lo que le entrega al registro electoral el acceso a sus datos para participar en el sufragio, refuerza los sistemas democráticos y participativos y los hace más eficientes.

Es lo ocurrido en marzo de 2018 en el país africano de Sierra Leona, donde se implementó tecnología *blockchain* en sus elecciones y, aunque solo fue parcialmente, alcanzó un 70% de los votos emitidos y se convirtió en un precedente para iniciativas a nivel mundial (Muñoz, 2018). La responsable tecnológica del proceso fue la empresa suiza Ágora.[12] Según declaraciones de Leonardo Gammar, de Ágora, *blockchain* permitió almacenar los votos de forma anónima y ofreció acceso en tiempo real a los resultados correspondientes de los votos emitidos por este sistema, para que cualquier parte interesada los revise, cuente y valide. En el

12 Ágora es un ecosistema de votación basado en *blockchain*, que permite a cualquier persona votar en línea, desde un dispositivo digital de una manera totalmente segura, fácil y verídica (https://www.agora.vote/about).

ámbito militar, podría ser aplicado junto con el uso de *Smart Contracts*, para que se otorgue automáticamente la autorización, en el caso que se requiriera para el empleo de efectivos o medios militares, en escenarios y condiciones establecidos previamente, como es el caso de una situación de emergencia nacional.

6.3 Comunicaciones

En noviembre de 2018, Telefónica[13] e IBM[14] anunciaron un acuerdo de colaboración para optimizar procesos de negocio propios del sector telecomunicaciones a través del uso de *blockchain*. La colaboración se enfocará en aspectos clave del *blockchain* que ayudarán a solventar procesos complejos y habituales en la prestación de servicios, ya que monitorizará, en tiempo real, la veracidad y trazabilidad de cada llamada internacional y sus atributos (principalmente el origen, destino y duración de la misma), en una plataforma descentralizada a la que todos los operadores participantes en el enrutamiento tendrán acceso (Telefónica, 2018).

En cuanto a las comunicaciones militares, al contar con protocolos P2P de la *blockchain*, de llegar a producirse un ataque que interrumpa los canales de comunicaciones principales como Internet, enlaces inalámbricos o satelitales, se podrían enviar mensajes mediante canales alternativos de radiofrecuencia de uso militar (HF, VHF, UHF).

La red de *blockchain* podría ser distribuida a lo largo del territorio en distintas unidades militares que cuenten con la suficiente capacidad técnica para alojar servidores *blockchain*, de tal manera que existiría una copia local del libro mayor en caso de producirse interrupciones en la red, la cual, al estar distribuida, no tiene un punto central vulnerable. El Departamento de Defensa de Estados Unidos planteó que contar con un sistema de mensajes y transacciones seguro es una necesidad crítica, junto con la condición de que este debe ser accesible a través de un navegador *web* o una aplicación nativa. Para lo anterior, la Agencia de Proyectos de Investigación Avanzados de Defensa[15] se encuentra en la búsqueda de soluciones

13 Telefónica S.A es una empresa multinacional española de telecomunicaciones, con sede central en Madrid, España, situada como la compañía de telecomunicaciones más importante de Europa y la quinta del mundo, con más de 346 millones de clientes.

14 Fundada en 1911, International Business Machines Corporation (IBM) (NYSE: IBM) es una reconocida empresa multinacional estadounidense de tecnología y consultoría con sede en Armonk, Nueva York. Fabrica y comercializa *hardware* y *software* para computadoras y ofrece servicios de infraestructura, alojamiento de Internet y consultoría en una amplia gama de áreas relacionadas con la informática, desde computadoras centrales hasta nanotecnología.

15 Conocida por su acrónimo DARPA o en su nombre original en inglés Defense Advanced Research Projects Agency, es una agencia del Departamento de Defensa de Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar.

que sean capaces de crear, transferir y recibir los mensajes utilizando una red de mensajería descentralizada (Darpa, 2018).

6.4 Autenticación de títulos

En el caso de instituciones que entregan títulos académicos o de formación, una vez que son registrados en la *blockchain*, estos quedan almacenados en la red y no pueden ser alterados o falsificados. Un ejemplo de esto, es el caso de Woolf University,[16] donde 14 investigadores de Oxford crearon el primer centro del mundo basado en *blockchain*, en el que los computadores controlan cada movimiento de la vida académica. De esta manera, nadie puede falsificar las notas o los títulos. Todos los movimientos académicos del alumno y del profesor se registran en tiempo real en miles de computadores repartidos por el mundo.

En un informe de la Comisión Europea publicado en 2017, sobre la aplicación de *blockchain* en educación (Grech & Camillery, 2017), se destaca que la *blockchain* permitiría verificar automáticamente toda la experiencia de aprendizaje de una persona sin la necesidad de contactar a la institución que emitió el título. El estudio menciona como aportes de esta tecnología: el control de las calificaciones, la acreditación, los pagos, el registro de los movimientos de los estudiantes o la propiedad intelectual, entre otros. Además, se destaca la inmutabilidad de los registros y la imposibilidad de modificarlos. De esta manera, por parte de las instituciones se podría evitar que personas que no cuenten con los títulos exigidos o presenten certificados falsificados sean contratadas.

6.5 Seguimiento de productos y cadena de suministros

En un informe de Rabobank Research,[17] titulado "*Blockchain*: The Trigger for Disruption in the Food Value Chain" (Rabobank, 2017), se plantea que para que las empresas logren tener éxito en la cadena de valor de los alimentos, deberían comenzar a explorar la forma de adquirir la tecnología *blockchain*, lo que se traduciría en reducir costos, aumentar la eficiencia y añadir aún más valor al trabajo.

16 https://woolf.university.

17 Rabobank (Coöperatieve Centrale Raiffeisen-Boerenleenbank B.A.) es una entidad financiera holandesa fundada en 1972 y de carácter multinacional. Proveedor mundial de servicios financieros para el sector de alimentos y negocios agrícolas, publica informes con estudios de las tendencias y desarrollos en la cadena alimentaria a nivel mundial.

Es el caso de Walmart,[18] que ya ha implementado el *blockchain* en su funcionamiento, lo que le ha permitido saber en tiempo real de dónde viene un producto, cuáles fueron sus condiciones de producción, cuál es su estado en el trayecto y cómo fue entregado en el punto de venta. De esta forma, mejoraron la trazabilidad de sus alimentos y lograron transparentar la red de suministro de sus productos. Este campo es de gran interés, en general, para la logística militar y, en particular, en lo referido al suministro de componentes del equipamiento militar.

En agosto de 2018, el presidente de Estados Unidos, Donald Trump, convirtió en ley un proyecto de defensa por 716.000 millones de dólares, que autoriza el gasto militar e incluye menores controles en los contratos del gobierno con ZTE Corp de China y Huawei Technologies Co Ltd.

En un informe publicado por la reconocida Fundación para la Defensa de las Democracias,[19] expertos de las agencias de inteligencia de Estados Unidos han dicho que les preocupa que ZTE, Huawei Technologies Co Ltd y algunas otras empresas chinas que estén en deuda con el gobierno chino, aumenten el riesgo de espionaje, debido a las posibles vulnerabilidades en las cadenas de suministro de equipamiento militar mediante la introducción de *hardware* malicioso, dado que en un posible escenario de conflicto, pueda verse alterado su correcto funcionamiento (Cummings, 2017). *Blockchain* sería la solución para esta vulnerabilidad, por su capacidad de seguimiento o trazabilidad, al establecer la procedencia de cada elemento utilizado en los sistemas (procesadores, circuitos o componentes). De esta forma, las instituciones de la defensa podrían gestionar de mejor forma la adquisición de componentes de los distintos proveedores, muchos de los cuales no cuentan con sistemas de control y seguridad que eviten futuros sabotajes. En consecuencia, cualquier cambio no autorizado en una cadena de suministros, por mínima que esta sea, sería detectada al instante evitando la incapacidad de no poder controlar los miles o millones de elementos que integran un sistema de armas moderno.

---

18 Wal-Mart, Inc. es una corporación multinacional de tiendas de origen estadounidense, que opera cadenas de grandes almacenes de descuento y clubes de almacenes. Es la mayor corporación pública del mundo, según la lista Fortune Global 500 de 2017. Cada semana, más de 275 millones de clientes y miembros visitan más de 11.300 tiendas en 58 banners en 27 países y sitios web de comercio electrónico en 10 países. Con ingresos en el año fiscal 2019 de $ 514,4 mil millones, Walmart emplea a más de 2.2 millones de asociados en todo el mundo.

19 La Fundación para la Defensa de las Democracias (FDD) es un instituto de investigación, que se centra en la seguridad nacional y la política exterior de Estados Unidos. Según lo indica en su sitio web, realiza una investigación en profundidad, produce análisis precisos y oportunos, identifica actividades ilícitas y brinda opciones de políticas, todo con el objetivo de fortalecer la seguridad nacional y reducir o eliminar las amenazas planteadas por adversarios y enemigos de Estados Unidos y otras naciones libres.

6.6. Energía

En este ámbito, *blockchain* permitiría que usuarios del sistema eléctrico, que pudieran generar electricidad por medio de energías renovables dentro de sus propias instalaciones, vendan directamente sus excedentes sin intermediarios. La generación de energías limpias, como la energía solar y eólica de forma descentralizada, permite a quienes las generan no solo aprovecharlas para su propio consumo, sino que además aportan al sistema central, gestionando de mejor manera la información sobre los precios, los activos y los acuerdos entre todas las partes que participan de la cadena energética. Este es el caso de Chile, en donde la Comisión Nacional de Energía está aplicando esta tecnología para publicar información y estadísticas como los precios medios de mercado, los factores de emisión, los costos marginales y las instalaciones de generación residencial, entre otros (Cne, 2018). El aumento de la capacidad de cómputo en una institución está asociado a la adquisición de una mayor cantidad de equipos de red, servidores y equipos terminales, entre otros, lo que significa, al mismo tiempo, una gran cantidad de consumo de energía eléctrica, por lo que se hace necesario hacer más eficiente el uso de los recursos.

6.7. Prevención de delitos

Blockchain puede ser una solución a los problemas de corrupción y operaciones fraudulentas como son las licitaciones públicas, las cuales serían asignadas de forma automática a las empresas que hayan sido los mejores oferentes y no a aquellas cuyos funcionarios hayan ofrecido algún tipo de incentivo extraoficial, ya que, por medio de los *Smart Contracts*, se puede establecer un control en contra de la manipulación de políticas, desviación de presupuestos, reglas de procedimiento en el financiamiento y/o en la asignación de recursos, fechas de pago, emisión de documentación, entre otros, por parte de aquellos que se encuentran en posiciones de toma de decisiones y de quienes abusan de dicha posición.

7. LA CUARTA REVOLUCIÓN INDUSTRIAL

La tecnología *blockchain*, unida a otros conceptos como son IoT, inteligencia artificial, automatización, *big data*, realidad virtual, entre otros, dan paso a la nueva revolución digital. La cuarta revolución industrial o también llamada industria 4.0, es la era que sigue a los otros tres procesos cruciales precedentes. La primera revolución, entre 1760 y 1830, dio el paso de la producción manual a la mecanizada, gracias a la aparición, por ejemplo, del motor a vapor. La segunda, alrededor de 1850, trajo la electricidad y permitió la fabricación en serie. La tercera llegó a mediados del siglo XX, de la mano de la electrónica, las tecnologías de la información y de las telecomunicaciones. El cambio

que caracteriza a la cuarta revolución industrial es que los sistemas de producción estarán basados en tecnologías inteligentes que trabajarán unidas y en línea, a través de Internet, con un nivel en sus procesos de tanta precisión, velocidad y eficiencia, que generará en los países un aumento nunca antes visto en la producción, a un costo sumamente más bajo.

Como es de suponer, una evolución en lo que se refiere a lo tecnológico y la producción, genera nuevas incertidumbres a nivel mundial. La primera es la insuficiente capacidad de adaptarse por parte de los países a asumir los desafíos propios del progreso industrial, lo que proyecta desalentadoras consecuencias en lo económico, social y político, al estimarse que la automatización generara un alto nivel de cesantía. Por otro lado, se plantea que los países que logren adaptarse a estos cambios, tomen una posición estratégica de liderazgo frente a los países que no tengan el mismo éxito, ya que, los primeros, podrían concentrar la producción y la riqueza, generando una suerte de "darwinismo tecnológico", donde aquellos que no se adapten no lograrán sobrevivir. Como consecuencia, es posible pensar que la industria orientada a desarrollar productos y servicios relacionados a la seguridad y la defensa centralizará sus esfuerzos en estrechar relaciones con los países que se levanten como potencias a nivel mundial, lo que implica nuevos desafíos para Chile en el ámbito de la defensa (Lodeiro, 2018).[20] Entre los desafíos más directos a enfrentar, está la desaparición de empleos por la sustitución de personas por robots en tareas administrativas, cadenas de montaje, entre otras. Por otro lado, los países sitúan sus prioridades con vista a la creación de empleos relacionados a la computación, lo que involucra un proceso educativo de capacitación y generar el capital humano calificado necesario para la nueva demanda de empleos.

El caso de Alemania es destacable, tal como muestra la Figura Nº 3. Para la canciller alemana Angela Merkel, es una necesidad crear y aplicar la tecnología de punta y adoptar el sistema de educación dual de Alemania [21], con la finalidad de asegurar mano de obra cualificada, ya que en su calidad de primera economía del viejo continente, desea seguir liderando en Europa y, para ello, quiere alcanzar en un par de años la total digitalización de su industria, con el objetivo de incrementar y estabilizar el ritmo de crecimiento de su PIB.

---

20 Andrea Lodeiro E. es Periodista (ARCIS), Magíster en Ciencia Política, Seguridad y Defensa (ANEPE), Diplomada en Estudios Políticos y Estratégicos (ANEPE) y graduada de los cursos de Administración de Recursos de Defensa y Coordinación Interagencial y Contraterrorismo (CHDS).

21 En el sistema de formación dual alemán, se prepara a los egresados de los colegios para la futura vida laboral. La formación técnica dura entre dos y tres años y medio, según el oficio y la formación escolar previa y se realiza en forma dual en dos lugares de aprendizaje: la teoría se enseña en las escuelas vocacionales y, la práctica, en las empresas de formación.

Figura Nº 3: Para Alemania la Revolución 4.0 es prioridad.

Fuente: Perasso, 2016.

8. CONCLUSIÓN

En la historia de la humanidad los avances tecnológicos son los responsables de acelerados y profundos cambios en lo económico y social. En la actualidad nos encontramos frente a una nueva revolución tecnológica, donde distintos tipos de desarrollo convergen y se unen para crear cosas inimaginables hasta hace unos años, incluso para los más visionarios. Los retos que nacen para los países a partir de esta revolución, generan distintos puntos de vista, tanto optimistas como pesimistas. Lo que está claro, es que para Chile son muchos los desafíos que debe enfrentar. No exento de dificultades, nuestro país ante esta nueva dimensión tecnológica debe potenciar su inversión en educación, investigación e innovación y desarrollo, lo que implica cambios en su modelo productivo, el impulso de nuevos esquemas de negocio, creación de nuevas industrias, entre otros. En palabras de Julio Pertuzé, "esta es una ola que viene y muy rápido (...) el primero que llega, termina ganando y nosotros queremos que el sector productivo chileno sea de los primeros que salga con estos nuevos usos (como la blockchain) a la conquista, no solo de Chile, sino que del mundo entero" (Pertuzé, 2018).

En este contexto, tecnologías como *blockchain* se convertirán en protagonistas de estos cambios radicales en los modelos de negocio y de gestión en las instituciones, al romper el paradigma de los modelos de gestión centralizados, transformando no solo la economía, la sociedad y las instituciones, sino que es importante considerar también cambios importantes en el sector defensa, donde las instituciones armadas

deben generar instancias para la inversión del desarrollo tecnológico y la investigación científica, aprovechando las oportunidades que aparecen a nivel tecnológico, para llegar potencialmente a convertirse en notables capacidades para sus funciones. No existen sistemas infalibles o que no sean vulnerables de alguna manera a ciberataques o al mal uso de estos, lo que puede dañar gravemente la imagen, la privacidad de los datos y la seguridad de las instituciones, razón por la cual se hace sumamente necesario buscar y poner en marcha soluciones como *blockchain*.

Es así como la presente revisión de distintos casos de uso de esta tecnología a nivel mundial, puede ser de interés para las instituciones encargadas de la defensa de Chile, con la finalidad conocer y, posteriormente, investigar sobre sus potencialidades y las posibles aplicaciones de *blockchain*, a través del seguimiento de los avances logrados en esta materia por otros países. Al mismo tiempo, puede servir como iniciativa para la creación de equipos de trabajo con expertos en la materia, con la intención de interactuar y recoger experiencias del desarrollo de aplicaciones en el ámbito civil y extrapolar su uso al ámbito de aplicación militar.

Finalmente, cabe destacar que la *blockchain* es una tecnología que dará mucho de qué hablar en los próximos años y que puede convertirse en un verdadero aporte a la solución de las vulnerabilidades existentes de muchos de los sistemas utilizados en la defensa. Así como los modelos de negocio y la gestión empresarial deberán adecuarse a los cambios venideros, la defensa también se verá en la obligación de romper el tradicional modelo de control centralizado y reemplazarlo por uno distribuido y descentralizado lógica y geográficamente.

BIBLIOGRAFÍA

24horas (30 de enero de 2019). Alcalde de Rapa Nui tras incendio en juzgado. “Era imposible razonar con los manifestantes, nos sobrepasó”. Recuperado de: https://www.24horas.cl/nacional/alcalde-de-rapa-nui-tras-incendio-en-juzgado-era-imposible-razonar-con-los-manifestantes-nos-sobrepaso-3051738

ABC Motor (27 de febrero de 2018). El móvil será la llave del Porsche del futuro. Recuperado de: www.abc.es/motor/reportajes/abci-movil-sera-llave-porsche-futuro-201802271212_noticia_amp.html.

BBVA (26 de abril de 2018). BBVA e Indra realizan el primer préstamo corporativo sobre tecnología ‘*blockchain*’ del mundo. Recuperado de: https://www.bbva.com/es/bbva-indra-realizan-primer-prestamo-corporativo-tecnologia-*blockchain*-mundo/

Cabrera, F. (2018). Tecnología *Blockchain*: elementos básicos, aplicaciones y marcos regulatorios. (9 de mayo de 2018). Santiago, Chile: Biblioteca del Congreso Nacional de Chile.

Cne (5 de abril de 2018). Ministra Jiménez lanza tecnología *Blockchain* en datos del sector energético. Recuperado de: https://www.cne.cl/prensa/prensa-2018/04-abril-2018/ministra-jimenez-lanza-tecnologia-*blockchain*-en-datos-del-sector-energetico/

Cummings, D. (11 de julio de 2017). FDD and CPRI Research *Blockchain* For Supply Chain Protection. Recuperado de: https://www.ethnews.com/fdd-and-cpri-research-*blockchain*-for-supply-chain-protection.

Defense Advanced Research Projects Agency (2018). DARPA Defense Advanced Research Projects Agency, 1958-2018. Official website. Recuperado de: DARA-PA60_publication-no-ads.pdf

Grech, A., y Camillery, A. (2017). *Blockchain in Education.* Luxembourg: Publications Office of The European Union. Recuperado de: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_*blockchain*_in_education(1).pdf

Perasso, V. (12 de octubre de 2016). Qué es la cuarta revolución industrial (y por qué debería preocuparnos). Recuperado de: https://www.bbc.com/mundo/noticias-37631834

Pertuzé, J. (1 de agosto de 2018). La apuesta del Gobierno por el *blockchain* para que Chile no se quede abajo del carro de la Cuarta Revolución Industrial. (Entrevista de P. Marchetti). Recuperado de: https://www.emol.com/noticias/Economia/2018/08/01/915332/La-apuesta-del-Gobierno-por-el-*Blockchain*-para-no-quedarse-abajo-del-carro-de-la-Cuarta-Revolucion-Industrial.html.

Preukschat, A. (2017). *Blockchain: La revolución industrial de internet.* Madrid, España: Grupo Planeta.

Samsung (12 de Julio de 2018). El Internet de las Cosas aterriza en el hogar y promete hacer la vida más fácil. Recuperado de: https://news.samsung.com/cl/el-internet-de-las-cosas-aterriza-en-el-hogar-y-promete-hacer-la-vida-mas-facil

SAP (26 de febrero de 2019). ¿Qué es Internet de las Cosas (IoT)? Recuperado de: https://www.sap.com/latinamerica/trends/internet-of-things.html

SMIT, H. (2017). *Blockchain*: The Trigger for Disruption in the Food Value Chain. Recuperado de: https://research.rabobank.com/far/en/sectors/farm-inputs/*blockchain*_the-trigger-for-disruption-in-the-food-value-chain.html

Telefónica (14 de noviembre de 2018). Telefónica e IBM colaboran para optimizar procesos del sector telco con *blockchain*. Recuperado de: https://www.telefonica.com/es/web/sala-de-prensa/-/telefonica-e-ibm-colaboran-para-optimizar-procesos-del-sector-telco-con-*blockchain*.

Workie, H. y Jain, K. (2017). Distributed ledger technology: implications of *blockchain* for the securities industry. En: *Journal of Securities Operations & Custody*, pp. 355-437. Washington, Estados Unidos: FINRA. Recuperado de: https://www.finra.org/sites/default/files/FINRA_*Blockchain*_Report.pdf.