INSTITUTO TECNOLÓGICO DE BUENOS AIRES – ITBA
MAESTRIA EN DIRECCION ESTATEGICA Y TECNOLOGICA
ESCUELA DE POSTGRADO

Blockchain una revolución de Internet, sus aplicaciones más allá de las monedas virtuales

Incorporación de Blockchain en Prefectura Naval Argentina y aplicación de Certificado de Altura de Ríos

AUTOR: Chambi Villarroel, Gudnar Darwin (Leg. Nº 104257)
DIRECTOR DE TESIS: Luzuriaga, Diego

TESIS PRESENTADA PARA LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN DIRECCION ESTRATEGICA Y TECNOLOGICA (ARGENTINA) Y MASTER EXCUTIVA EN DIRECCION ESTRATEGICA Y TECNOLOGICA (ESPAÑA)

Agradecimientos

Agradezco a mis compañeros de trabajo y todos los que me colaboraron en el proceso de acabar un ciclo de aprendizaje en la Maestría junto a la realización de este trabajo:

A los docentes del ITBA por sus enseñanzas durante el posgrado.

A mi tutor Diego Luzuriaga por su tiempo, sus aportes y orientaciones.

Al Ing. Mariano Musante y el Dr. Cristian Castello por toda su colaboración y tiempo.

A todo el personal de BFA , NIC Argentina ,CABASE ,el Boletín Oficial de la República Argentina y Dirección General de Sistemas Informáticos de la Secretaría Legal y Técnica por el aporte, tiempo y colaboración.

A la Prefectura Naval Argentina por los años de trabajo que me permitió seguir avanzando con mi carrera profesional para proponer ideas y estrategias de mejora tecnológica dentro la Institución.

Dedicatoria:

A mi Familia por el apoyo incondicional de afrontar desafíos en la vida y seguir mejorando tanto en lo humano como en lo profesional

Y a toda organización o persona interesada a incorporar el nuevo paradigma de blockchain y esperando que el presente trabajo sea de ayuda en las transformaciones digitales

Índice Capítulos:

Índice de Cuadros:

Índice de Figuras:

Abstract:

La aparición del Internet fue una revolución en el acceso y difusión de la información en todo el mundo, luego apareció el *Bitcoin* con su base tecnológica llamada *Blockchain* y en consecuencia aparecieron otras criptomonedas y el sector económico es el que más vino desarrollando usos en la cadena de bloques. Y los expertos afirman que el *Bitcoin* es solo la punta del *iceberg* del potencial de aplicaciones con la tecnología *blockchain*, considerándose de esta forma la presencia de otra revolución de transmisión y valor en los datos en las redes, pasando de la Internet de la información al Internet del valor.

En este trabajo se clasifican, analizan e identifican los casos de uso más allá de las criptomonedas, resaltando la importancia dentro el sector público a los países que vienen incorporando esta innovación tecnológica de cadena de bloques. También se identifica la importancia de que un organismo público incorpore *Blockchain* con aplicaciones para simplificar y agilizar toda clase de registros en forma descentralizada, segura y distribuida, siendo así un nuevo paradigma de la forma de registrar datos.

Luego se analiza, describe y explica de cómo ser parte de una plataforma *blockchain* en Argentina para desplegar aplicaciones y realizar transacciones en forma gratuita, donde se requiera menos capacidad de cómputo para la generación de bloques y no está orientada a la moneda virtual, diferenciándose de los modelos tradicionales de las criptomonedas que están basados en la competencia entre sus nodos para realizar transferencias monetarias. La plataforma argentina va estar integrada por múltiples partes interesadas como el sector público, privado, académico y de la sociedad civil.

Y en particular se demuestra a la Prefectura Naval Argentina como una de las primeras autoridades marítimas en usar una red *Blockchain* con un caso de uso como el Registro de Altura de Ríos haciendo más confiable, seguro y transparente la información para el navegante o cualquier otro organismo que requiera saber el estado de las aguas y así mostrando la autenticidad de sus documentos registrados.

Introducción

Relevancia

En los años setenta en Estados Unidos se desarrollaba el Internet de la información a partir del sector militar y académico, luego se masificó su uso en todo el mundo hasta el día de hoy, donde se conectan muchas personas y todo tipo de entidades para acceder a la red ,esto impactó en la forma de relacionarnos en nuestra vida. Ahora con la iniciativa del sector financiero en este siglo XXI se habla de la Internet del valor con la aparición de *Blockchain* con el *Bitcoin* (Nakamoto,2008) considerada como otra revolución o un nuevo concepto de Internet porque permite compartir y gestionar el valor de activos o bienes digitales sin la dependencia de una entidad central de confianza que centralice el proceso.

Con *Blockchain* también se extiende a compartir valor como títulos, registro, archivos, certificaciones o canciones de una manera digital y descentralizada sin requisito de alguien para imponer criterio a los participantes. Esta capacidad de esta nueva tecnología resulta algo apasionante y puede revolucionar la forma de entender el mundo, impactando en muchos sectores de la industria, gobiernos y del sector económico.

El tema de la cadena de bloques debe ser de importancia de estudio porque es una revolución de Internet, siendo una nueva tecnología de interés en las transformaciones digitales de las organizaciones. Existen hoy en día muchas plataformas de *blockchain* diferenciándose en la forma de generar el bloque.

Blockchain presenta una red descentralizada, permitiendo registros de transacciones y estas se vayan guardando en forma distribuida en varios sitios diferentes, siendo así una infraestructura confiable, transparente e íntegra. También cuenta con métodos criptográficos para evitar modificaciones de los registros en esta tecnología comportándose como un libro contable digital y seguro.

Y es sumamente importante que en Argentina se haya conformado una iniciativa de una red *blockchain* en el año 2018 llamada Blockchain Federal Argentina, en el cual he participado en este proyecto donde también participaron distintos organismos públicos y

privados, pude asistir a reuniones técnicas y administrativas. También estuve presente en eventos, conferencias y charlas de temática *Blockchain*.

Definición y alcance del problema:

Con la plataforma de Internet de la Información establecida en todo el mundo y su uso masivo, luego surge *Bitcoin* con la base tecnológica de la cadena de bloques, revolucionando al Internet del valor, cambiando el concepto de centralizar los datos en la red, existiendo en la actualidad una variedad de plataformas y aplicaciones en *blockchain.*

En este trabajo se describen, analizan y clasifican las distintas plataformas de *Blockchain* con sus atributos y las aplicaciones involucradas en distintos sectores para que luego podamos optar por implementar la cadena de bloques en un organismo público.

Se va analizar y explicar de como un organismo público puede implementar una red *Blockchain*, integrada por los sectores en Argentina de la Industria y Comercio, Academia, Sociedad Civil, Gobiernos Provinciales, CABA y Administración Pública Nacional.

Se usarán herramientas de implementación en un entorno de desarrollo como *Visual Studio Code* para analizar la generación de bloques y el despliegue de los *Smart Contracts* en las plataformas de *Blockchain*.

Estado del conocimiento:

Antes de la aparición del *Bitcoin*, desde los 90 hubieron movimientos sociales y filosóficos y se los denominaba los *cipherpunk*, venían con la idea de la seguridad y autonomía en la información de Internet, fue así que ya se focalizaba en la idea descentralizada de los datos en Internet.

Luego del *Bitcoin* (Satoshi Nakamoto, 2009) , aparecieron otras criptomonedas como *Litecoin* , *Ripple*, *Dash* , después surgió la aparición de *Ethereum* y los contratos inteligentes (Buterin, 2014) que lleva hasta hoy en explorar las ventajas del uso de este nuevo paradigma de la cadena de bloques, el cual comprenden el estudio más allá de las

monedas virtuales y por ejemplo según IBM en su sitio lo menciona en distintos sectores como Sector público , Automoción , Banca y servicios financieros, Sanidad, Entretenimiento y Medios, Comercio minorista y Bienes de consumo , Viajes y Transportes ,Cadena de suministros y Seguros.

Dentro del sector público es de importancia el uso de *blockchain* por las características intrínsecas de esta tecnología tal como la transparencia, la inmutabilidad y la garantía de la información, son factores que ayudarán dentro de la administración pública a garantizar la confianza de los ciudadanos en los procesos administrativos.

Y además varios países están a la vanguardia e invirtiendo en proyectos de *Blockchain* tal como Inglaterra, Suiza, Singapur y Estados Unidos a nivel corporativo, gubernamental y emprendedor (Preukschat y Molero Manglano,2017).

.

El gobierno del Reino Unido estuvo subvencionando en proyectos sustentados en la *blockchain*, entendiendo el potencial de esta tecnología asegurando el actual estatus de Londres como referencia mundial en gestión de servicios financieros (Álex Preukschat e Íñigo Molero Manglano (2017).

En Suiza cerca de Zurich se organizó un ecosistema para inversiones de tecnología *blockchain* conocida popularmente como *Crypto Valley* siendo una asociación independiente establecida para el desarrollo de criptomonedas y *blockchain* contando con el apoyo del gobierno suizo, cuenta con leyes que favorecen seguridad jurídica a los emprendedores ,atrayendo el talento.

En Estados Unidos se vino invirtiendo en un capital importante para el impulso de *blockchain.* Las empresas e inversores de *Silicon Valley* apuestan en las *blockchain* públicas como *Bitcoin* o *Ethereum*, con la espera de triunfar tal como fue antes con el Internet de la información. Y en *Wall Street* prefieren trabajar sobre todo en las *blockchain* privadas porque consideran que un modelo de negocio regulado tiene mejor cabida.

En Singapur impulsaron la tecnología *blockchain* desde las administraciones públicas, empresas privadas, los académicos y los desarrolladores. Logrando coordinar con los

distintos sectores sociales la fundación del centro de innovación IBM de blockchain con sede en esta ciudad - Estado asiática. Singapur con seguir invirtiendo en la tecnología de la cadena de bloques, tiene su intención de seguir formando parte de los países líderes del mundo en este siglo XXI.

La cadena de bloques es la columna vertebral del *Bitcoin*, siendo una tecnología muy atractiva para resolver problemas comerciales financieros y no financieros actuales.

Aplicaciones de la tecnología *blockchain* dentro del sistema financiero:

- Con el uso del *blockchain* se abre la posibilidad de agilizar los pagos, transferencias y el envio de remesas abaratando mucho su costo, como ejemplo desde el 2015 la *startup Abra* viene desarrollando un sistema digital global de gestión de activos basado en *blockchain* de *bitcoin* permitiendo el envio prácticamente instantáneo de remesas a otros países desde el móvil celular.
- En el Mercado de valores, *Nasdaq* viene desarrollando desde Octubre del 2015 el uso de *blockchain* para el intercambio de acciones en su mercado de valores privado.
- En el 2015 dentro de lo que son los Mercados de predicción descentralizados, se encuentra *Augur* , un mercado de predicción descentralizado que permite a usuarios vender y comprar acciones anticipándose a un suceso en función de la probabilidad de que se produzca algún desenlace.
- En Agosto de 2016 el informe del Foro Económico Mundial afirma que la tecnología *blockchain* alterará de raíz el modo en el que las instituciones financieras hacen negocios y acabará por convertirse en el corazón del sistema financiera internacional. El 80 % de los bancos ha reconocido estar trabajando ya en el desarrollo de productos basados en la cadena de bloques.
- En Septiembre de 2016, IBM realiza una encuesta donde los resultados son que los bancos y las empresas financieras están con el interés de implementar la tecnología *blockchain* y sacar al mercado servicios comerciales.

Aplicaciones posibles de la tecnología *blockchain* en otros ámbitos no financieros:

- Sector de Seguros (Gonzalo Gómez Lardies y Daniel Díez García,2017)
- Telecomunicaciones (Christoph Steck y Eusebio Felguera Garrido,2017)
- Sector energético (Ignacio Madrid Benito,2017)
- Farma y salud (Dioni Nespral,2017)
- Medios de comunicación (Covadonga Fernández González,2017)
- ONG (Íñigo Molero Manglano,2017)
- Sector público (Roberto Fernández Hergueta,2017)
- Industria 4.0 (Óscar Lage Serrano,2017)
- Internet (Covadonga Fernández González,2017)

Luego fueron apareciendo más *blockchain* públicas, privadas y las hibridas, la tendencia es que la banca e instituciones financieras prefieren las *blockchain* privadas por un tema de confidencialidad en la información que manejan, en cambio grandes empresas como en *Sillicon Valley* y los grandes corporaciones de Internet optan por las *blockchain* públicas, donde aparecen las *Fintech* e *Insurtech*. En fin se abre a un amplio e infinitas ideas de aplicar *blockchain* con distintos casos de uso pero queda un largo camino para masificar el uso de la cadena de bloques así como lo fue el uso de las computadores personales o la telefonía celular, esta tecnología trae un cambio tecnológico, cultural y social. (Álex Preukschat,2012).

El hecho de usar criptomonedas y contratos inteligentes, queda el desafío por delante de regular el valor de la moneda virtual y sea legal su uso. Y los contratos inteligentes en un futuro tengan validez jurídica.

Hipótesis

La implementación de *Blockchain* en el sector público tiene un potencial enorme para aportar valor agregado en los procesos de registro.

Metodología

El desarrollo de este trabajo se corresponde con el estudio de caso.

El estudio de caso en *Blockchain* es un fenómeno singular, tiene complejidad, hay disponibilidad de usar la cadena de bloques en otros casos que van surgiendo en distintas áreas y es un potencial de aprendizaje para entender esta tecnología de innovación porque transforma las organizaciones.

Se toma en cuenta al autor Yin el cual considera el estudio de caso "no tiene especificidad, por lo que puede ser usado en cualquier disciplina para dar respuesta a preguntas de la investigación para la que se use" (Yin, 1993) y en este trabajo se lo clasifica dentro el ámbito tecnológico. También se toma en cuenta a Hernández (2006,p. 223-224) que considera los estudios de caso junto a procesos descriptivos para analizar profundamente el fenómeno para probar la hipótesis, abarcando el concepto de Yin.

Revisión bibliográfica

Se consultan libros, informes, *papers* y material *online* publicados en internet. También se toman en cuenta el interés de *stakeholders* en artículos de noticias en la web por la implementación de *Blockchain* en varios procesos dentro de organizaciones. Además se tuvo mejor conocimiento de esta innovación en la participación de reuniones técnicas y administrativas del Proyecto Blockchain Federal Argentina.

Objetivos generales:

Implementar *Blockchain* en una Organización pública como la Prefectura Naval Argentina para lograr un proceso de registro de datos descentralizado.

Objetivos específicos:

- Estudiar la bibliografía de *Blockchain*.
- Identificar plataformas y casos de uso en *Blockchain*.

- El Organismo público como la PNA cuente con la capacidad técnica de infraestructura de unirse a través de un nodo a la red de Blockchain Federal Argentina (BFA),convirtiéndose así en la primer fuerza con esta tecnología innovadora.
- Acordar para ser miembro a la red nacional Blockchain Federal Argentina.
- Participar en las políticas de uso de la red de nodos de BFA.
- Probar técnicamente que el nodo sellador y nodo transaccional estén operativos.
- Realizar la aplicación de Altura de Rios sobre la plataflorma multiservicios *blockchain* BFA.

Limitaciones y restricciones:

Actualmente existen muchos protocolos de consenso en *blockchain*, en este trabajo se analizarán la generación de bloques en los modelos de consenso Prueba de Trabajo o Prueba de Autoridad.

El entorno de pruebas de concepto de *blockchain* estará integrado en el entorno de *Visual Studio Code* contando con herramientas de lenguaje de *Solidity* para *Smart Contracts* y redes como *Ganache* y *Remix*.

La plataforma definitiva estará conformada por organismos y usuarios que pertenezcan a Argentina y quieran formar parte de la red nacional *Blockchain*.

Se almacenarán solamente los *Hashes* en la plataforma de *Blockchain* nacional con el modelo de consenso Prueba de Autoridad para no comprometer la información o archivos de las partes integrantes de la red.

Articulación:

El capítulo 1 describe el marco teórico de como surgió el Internet de la Información y su masificación a usuarios en todo el mundo. Luego se describe la revolución de Internet con el *Blockchain* pasando a llamarse el Internet del valor. Se describen las características y

funcionamiento que presenta *blockchain*. También se describen las distintas plataformas de *blockchain.*

El capítulo 2 describe los casos de uso en *blockchain* clasificando en financieros y no financieros. Haciendo hincapié del caso de uso para registro de documentos y de gran importancia en la administración pública.

El capítulo 3 se explica la implementación de *blockchain* en una organización pública, en particular a la Prefectura Naval Argentina con esta nueva tecnología y el caso de uso de registro de documentos como Altura de Ríos.

El capítulo 4 se analiza la importancia de *blockchain*, su evolución y sus riesgos.

Y por último en el capítulo 5 se llega a la conclusión del potencial de *Blockchain* en el sector público. Además de la importancia para la organización pública contar con una *blockchain* registrando documentos con transacciones sin costo.

También se describe en el Anexo el interés de *stakeholders* en artículos informativos y eventos.

Capítulo 1. Marco Teórico

1.1 Historia de Internet

Desde la antigüedad se almacenan y se accede a todo tipo de información, a través de libros en bibliotecas o también existieron registros de censos, cosechas entre otros ejemplos más. Se necesitaba entonces algún mecanismo para almacenar mucha información en cantidad y con el tiempo mejorar el acceso para varios usuarios a la información almacenada.

En 1884 Herman Hollerit desarrolló las tarjetas perforadas como uso de almacenamiento de información en un censo. Luego en la década de 1950 aparece la cinta magnética para el registro de datos en forma secuencial. Hollerit fue también en un futuro uno de los fundadores de IBM.

En la década de 1960 aparece el concepto de base de datos conjuntamente con la informática y las computadoras para el acceso al dato haciendo uso de discos . Aparecen sistemas de base de datos junto a lenguajes de programación. Un logro principal fue la alianza de IBM y *American Airlines* para el desarrollo de SABRE, un sistema operativo que manejaba transacciones e informaciones de los pasajeros de la compañía *American Airlines*.

Existió en ese entonces un consorcio llamado CODASYL (*Conference on Data Systems Languages*) que pertenecían a industrias e instituciones gubernamentales que se relacionaban con el proceso de datos, el objetivo principal era promover un análisis, diseño e implementación de los sistemas de datos más efectivos. Más adelante no se llegaron a establecer en un estándar fijo sino que lo llevó a cabo por ANSI.

1.1.1 Evolución de Internet en el mundo

El inicio de internet surge finales de los años 60 impulsado por el Departamento de Defensa de los Estados unidos y luego en 1969 en el mismo país estadounidense se constituye ARPANET (Red de la Agencia de Proyectos de Investigación Avanzada) para

la investigación de intercambio de datos entre computadoras. Se empezaba a trabajar en esa época en documentos llamados RFC (*Request for comments*) para definir protocolos, métodos,conceptos y programas relacionados con Internet.

En 1970 surge INTERNIC que fue un equipo coordinado por Jon Postel en el Instituto de Ciencias de la Información de la Universidad del Sur de California con el propósito de cómo administrar los recursos de la red que se iba desarrollando con el uso de direcciones de IP.

Luego INTERNIC pasó a ser reconocido como IANA(Autoridad de Números Asignados en Internet) siendo una organización responsable para avanzar en el modelo de administración de recursos de Internet. Luego en 1972 este organismo fue contratado por el Departamento de Defensa de Estados Unidos para que tomen la responsabilidad de registrar e identificar las universidades con posesión o administración de rango de direcciones IP,protocolos y nombres de dominios.

En 1973 se desarrollaron las primeras versiones de TCP/IP(protocolos de Internet) , este protocolo evolucionó hasta que en 1983 se estableció el IPv4 , también se fueron creando otros protocolos o aplicaciones como el FTP, el SMTP y el POP , permitiendo el intercambio de correos electrónicos y de archivos.

En Estados Unidos la *National Science Foundation* trabajaba en una red propia, que luego años mas tarde en 1986 se creó la NSFNet que se constituyó como el *backbone* de Internet a nivel mundial. También ese mismo año estaba el IETF (Grupo de Trabajo de Ingeniería de Internet) una entidad a nivel internacional encargada de la regulación de propuestas y los estándares de Internet plasmados en documentos para contribuir a la Ingeniería del Internet.

Fue así que se dió inicio al desarrollo de diferentes protocolos y procedimientos para el armado de red y que permita ir construyendo nuevos protocolos sobre el TCP/IP y que en un futuro seria la red de redes llamada Internet como un modelo en capas y estándares abiertos.

En los 90 nace la tercera generación de base de datos que está orientada a objetos que vino de la mano de *Microsoft* y a lo que también se suma en esta década el auge del Internet que también facilitó el acceso a datos a través de la red mundial. Se desarrollaban también otras tecnologías como la telefonía celular y entre otras más que hacían en conjunto al desarrollo de las telecomunicaciones.

Estaban entonces tres compañías dominando el mercado de las bases de datos con IBM ,*Microsoft* y *Oracle.* Y *Google* como la compañía que genera gran información en el campo de Internet.

Hoy en día hay mucha variedad de *software* para manejar y crear base de datos con gran facilidad, y así *Windows* tiene un entorno de desarrollo llamado *Visual Studio* para integrar todo lo relacionado con programas de bases de datos, creación de páginas webs y aplicaciones.

La Historia de las base de datos viene acompañado de la evolución de la informática llegando al Internet de la información como plataforma para el acceso de todo el mundo a una gran cantidad de datos.

Internet es de mucha importancia y es una gran red que interconecta más redes y es una plataforma para la gestión de base de datos, por eso es de relevancia conocer como ha sido la evolución de Internet en el mundo y en Argentina.

Para el logro de interconectar redes se necesitaba hacerlo a través de un lenguaje común para que la comunicación sea en toda la gran red, garantizando la conectividad entre todos los dispositivos. Se definió así el *TCP /IP* (del inglés *Transmission Control Protocol/Internet Protocol*) el lenguaje de comunicación utilizado en Internet y fue desarrollado por *Vinton Cerf* y *Robert E. Kahn* durante la década del setenta.

El *TCP/IP* es un modelo que define las características de un conjunto de reglas para garantizar la conectividad de un extremo a otro en la red de Internet para el envio de datos desde una dirección origen a otra dirección destino.

Para dar un orden de cómo conectar a todas las redes del mundo, se estableció a través de IANA un orden de registros de direcciones llamadas IPs y números de sistemas autónomos ASN como identificadores de red para cada organización que haga uso del Internet.

IANA administra en forma centralizada los recursos numéricos de Internet, como los espacios de direcciones IP y los ASN.

También existen cinco RIR (Registros Regionales de Internet) que reciben las asignaciones de recursos numéricos de IANA.

Los *RIR* y sus regiones de incumbencia son mostrados en el siguiente gráfico Figura 1.1 :

Figura 1.1: Registros de Internet en el mundo

Fuente: Documento de Gestión de Redes, Módulo 1. LACNIC (2019)

La secuencia de asignación es comenzando de *IANA* donde se asigna el espacio de recursos numéricos a cada *RIR* y luego estos registros realizan asignaciones en sus respectivas regiones.

En la imagen anterior en el mapa puede distinguirse a *LACNIC* que es el Registro Regional para América Latina y Caribe, este recibe recursos numéricos de *IANA* y los asigna a su región

LACNIC es así una organización no gubernamental internacional que se estableció en Uruguay en el 2002 para la contribución al desarrollo de Internet en la región a través de una política activa de cooperación, promoviendo y defendiendo los intereses de la comunidad regional, colaborando en la generación de condiciones para que Internet sea un instrumento efectivo de inclusión social y desarrollo económico de América Latina y el Caribe.

LACNIC es administrada y dirigida por un una dirección de siete miembros elegidos por sus asociados, más de siete mil entidades de operación de redes, brindando servicios en 33 territorios de América Latina y el Caribe.

1.1.2 Internet en Argentina

En Argentina la evolución de Internet fue desde las universidades a ser un auge en distintos sectores.

En 1985 con la creación del Departamento de Computación de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires, un equipo comenzó a trabajar por primera vez en la investigación y el desarrollo de redes. Y luego crearon lo que luego se conocería como el proyecto Red Académica Nacional o RAN para conectar las instituciones académicas.

También se habían comenzado las primeras pruebas del protocolo X25(es un estándar para redes), en ese entonces era usado para la transmisión de datos. Hubo una iniciativa con el laboratorio de redes basadas en el protocolo UCCP (protocolo de comunicaciones). Fue así que estos sucesos se convirtieron en el inicio del surgimiento y desarrollo de internet en Argentina.

En los comienzos de 1987 en Argentina se logró establecer una conexión con la Universidad de Toronto de manera electrónica, esto fue la primera comunicación internacional por correo electrónico vía el protocolo UUCP(*Unix to Unix Communication Protocol*).Un trabajo en conjunto que se dió desde 1986 con la incorporación de Alberto

Mendezon , un experto en base de datos e inteligencia artificial proveniente de Canadá que se había integrado a la Cancillería argentina.

Se había acordado en ese entonces que la Red Académica Nacional recibiera todos los correos electrónicos de carácter académico y la Cancillería era el medio para la gestión de los envíos al exterior. Así de esta forma la Cancillería utilizaba la red para el intercambio con las embajadas. Y de la Cancillería a la Universidad de Toronto y luego la conexión al mundo.

La RAN (Red Académica Nacional) fue creciendo con más incorporaciones de Facultades teniendo a un servidor central de correo en la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires que se conectaba con Cancillería para transmitir los mensajes a las redes internacionales. Argentina llegó a establecer con más de 800 instituciones conectadas a través del correo electrónico.

Paralelamente en 1986 se intentó unir a las Universidades nacionales a través del proyecto RUTA(Red Universitaria Teleinformática Argentina) que consistió en implementar una red BITNET (red informática cooperativa de universidades de los Estados Unidos) nacional de misma tecnología de Estados Unidos.

La red BITNET se descontinuó en Argentina entre uno de los motivos porque en el mundo prospero Internet como el modelo a seguir con facilidad de hacer crecer la red usando PCs como los nodos de correo electrónico.

Luego se llegó a establecer el estándar TCP (*Transmission Control Protocol*) con el uso de direcciones IP (*Internet Protocol*) como identificadores junto al uso del archivo conocido como *HOST.TXT* , que se trataba de un listado en donde a un host era asociado a una IP , logrando en todo el mundo una forma de administración de forma manual de los nombres mapeados a números.

Con el crecimiento de Internet se pasó de la metodología de archivo *HOST.TXT* a la implementación de un nuevo modelo que se llamó Sistema de Nombres de Dominio (*Domain Name System*) que permitió el armado de un esquema distribuido de dominios

genéricos (gTLDs) tales como ".com",".mil" y ".edu" y los dominios de primer nivel geográfico como ".ar", ".cl" y "br".

La Cancillería siguiendo el proceso de transición al modelo de DNS (*Domanin Name System*), el 20 de Agosto de 1987 solicitó el registro de Dominio de Nivel Superior para la República Argentina , utilizando como código dos letras AR con el estándar ISO-3166-1, ISO (Organización Internacional de Normalización) este proporciona códigos para los nombres de países y otras dependencias administrativas .Luego el registro oficial se hizo efectivo el 23 de septiembre de 1987 y a través de un acuerdo con la Facultad de Ciencias Exactas y Naturales , se había comenzado a usar direcciones de correo electrónico como las que se usan actualmente. Esto fue un hito importante en el país en la historia del Internet para la Argentina con la creación del .ar porque se permitieron empezar a registrar los primeros nombres de dominios con la impronta nacional. El uso del .ar fue la base para que luego existiera NIC Argentina.

Hasta 1990 se continuó con el uso del correo electrónico, sumándose más organismos como la Secretaria de Ciencia y Tecnología y también la Organización Panamericana de la Salud.

Y en 1990, la Cancillería logra el establecimiento del primer enlace analógico con el uso del protocolo UUCP para el intercambio de mensajes y luego en corto tiempo también se logró establecer la conectividad TCP/IP con Internet. Así se iniciaron los inicios del Internet en Argentina.

En todo el mundo fue cada vez más el interés de distintos sectores en Internet. Y en 1991 se creó la *Internet Society* (ISOC) esta es una organización no gubernamental sin fines de lucro dedicada al desarrollo mundial de Internet. ISOC hasta el día de hoy continúa y luego con la aparición de debates sobre la evolución de internet excedió el ámbito académico porque se fueron involucrando más interesados, luego apareció el concepto de Gobernanza de Internet para la referencia a temas de discusión.

En el año 1992 se creó el Centro de Comunidad Científica de la Universidad de Buenos Aires que tuvo la responsabilidad de construcción de una red de la UBA(Universidad de

Buenos Aires) para conectar a todas las Facultades. Y en 1993 se formalizó la red de correo electrónico en toda la universidad y también se armó una red metropolitana con el uso del protocolo TCP/IP con una velocidad de 64 Kb. El 8 de abril de 1994 se dió la primera conexión digital a Internet en Argentina donde se logró la conexión a todo el sector académico , y con la posesión de la administración del dominio ".edu.ar" que tenía la Universidad de Buenos Aires ,luego años después quedó en manos de la Red de Interconexión Universitaria (RIU).

En los primeros meses de 1994 se fundó NIC Argentina dentro del ámbito de la Cancillería y luego empezó a funcionar como organismo reglamentado y con facultades para la registración de los dominios ".ar".

Y en noviembre de 1994 se constituyó la Red de Interconexión Universitaria impulsado por el Ministerio de Educación, con el objetivo de expandir la red a todas las universidades públicas del país. Hasta el día de hoy RIU continúa funcionando para mejorar su conectividad.

Otro acontecimiento importante de Internet fue en abril de 1995 donde la expansión de la red traspasó el ámbito académico llegando al área comercial, aumentando así la cantidad de usuarios.

Surgieron en el país las empresas proveedoras de servicios de Internet para todo tipo de usuarios como particulares, organizaciones y empresas. Luego surge CABASE ,esta es la Cámara Argentina de Internet que agrupa a distintos ISP(*Internet Services Providers*).

La red fue creciendo en CABASE incorporando nuevos miembros , con estas nuevas incorporaciones se fue formando una red de Puntos de Intercambio de Tráfico o *IXP* (*Internet Exchange Points*) en distintos puntos de la región Argentina para el intercambio de tráfico de distintas entidades como *ISPs* (Proveedores de Internet) , organismos gubernamentales, universidades y entre otros más. Se formó un ecosistema de miembros con el objetivo de tener mejor calidad en las comunicaciones, disminuir el costo y lograr la optimización de la velocidad y disponibilidad del servicio de Internet hacia el usuario final.

Además en CABASE se agregaron servidores Caché (hardware o software que guarda datos para que las solicitudes futuras de esos datos se puedan atender con mayor rapidez) de Distribución de Contenidos (*Content Delivery Networks*) y servidores caché *Google* , esto como una estrategia de ir guardando el tráfico de datos internacional en forma local a la red CABASE para un acceso mucho más rápido a que ir a buscar directamente el contenido fuera del país.

Actualmente el mundo del Internet se centraliza en la información de *Google*, *Facebook* y *Amazon*, siendo estas grandes corporaciones las que dominan la red de redes.

En forma paralela conforme se iba conformando la evolución de las redes desde los 60, había un movimiento filosófico y social sobre la privacidad de la información y la seguridad en las comunicaciones. En los 90 ya se venía pensando en la descentralización , un movimiento llamado *cipherpunk* dió lugar al origen de optar por el dinero digital anónimo, entre uno de ellos como ejemplo apareció de la mano de David Chaum quien fundó *Digicash*, se trataba de dinero digital , el desarrollo de código no era abierto , grandes compañías querían saber del código para una posible mejora y sea adaptable a distintos casos, *Digicash* entró en banca rota.Y en 2004 siguiendo la línea del movimiento de descentralización se estableció un protocolo de descentralización llamado *Proof of work* de la mano de Hall Finney, desde ese entonces se pensó en una criptografía segura y mejorada, Finney colaboraría en la prueba de transacción con Satoshi Nakamoto en lo que sería la primer criptomoneda cedida a Hall.

1.2 Aparición de Blockchain

1.2.1 Red Bitcoin, características y funcionamiento

EL 31 de Octubre de 2008, un grupo o individuo bajo el nombre de Satoshi Nakamoto publicó un *paper* con el título de "*Bitcoin: A Peer-To-Peer Electronic Cash System*". Este documento describe una versión electrónica de *peer to peer* de intercambio monetario sin la intervención de una institución financiera. El autor de este documento sigue siendo anónimo.

Bitcoin fue la primera realización de este concepto de intercambio de moneda virtual. Hoy la palabra criptomoneda está asociada a toda red y medio de intercambio donde se usa criptografía para hacer más seguras las transacciones y no estar usando un sistema con transacciones donde requieren de una identidad centralizada para la seguridad.

El 3 de Enero de 2009 fue implementado un programa *open source* con un nuevo protocolo, este generó un bloque inicial llamado bloque *Génesis* de 50 monedas virtuales de *bitcoins*. Desde entonces cualquier usuario puede instalar el programa *open source* y ser parte de la red *Bitcoin*. Esta red fue creciendo en popularidad hasta el día de hoy. Siendo así *Blockchain* la base tecnológica del *Bitcoin*, convirtiéndose en una tecnología innovadora y disruptiva con un amplio campo de investigación comparada en los comienzos cuando nacía Internet.

Cronología de la aparición del *Bitcoin*:

2008:

- 18 de Agosto fue registrado el nombre de dominio "*bitcoin.org*"
- 31 de Octubre se publicó el documento del diseño del *Bitcoin*
- 9 de Noviembre, el proyecto Bitcoin fue registrado en *SourceForge.net*

2009:

- 3 de Enero se genera el primer bloque llamado *Génesis* a las 18:15:05 GMT
- 9 de Enero se estableció la versión de *software Bitcoin* v0.1 disponible al público
- 12 de Enero se establece la primera transacción de *Bitcoin* , registrada en el bloque 170 donde Satoshi envía *bitcoins* a otro usuario llamado Hal Finney

Red descentralizada y distribuida

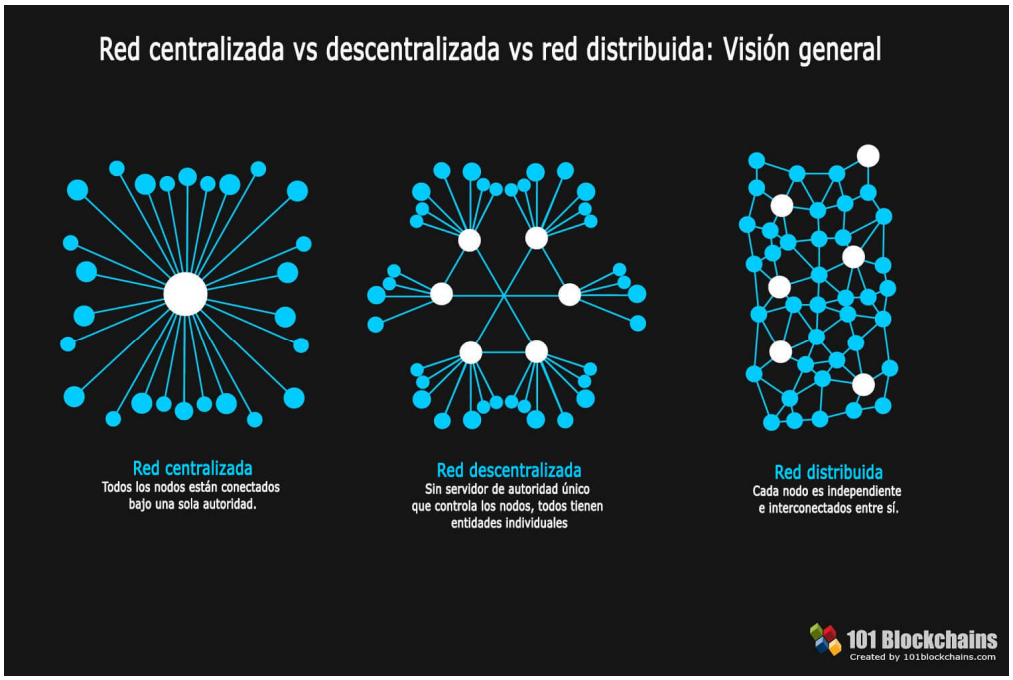
La red de *Bitcoin* es distribuida porque la información de transacciones es copiada en todos los nodos que la conforman, siendo así llamado también como libro contable distribuido. Y también es descentralizada porque no se requiere de un intermediario como autoridad central para validar las transacciones sino que todos los nodos de la red pueden participar

de la validación para aprobar las transacciones y sean agregadas a la cadena de bloques para luego estas pasen a ser inmutables.

Blockchain se diferencia así de un registro central o todo medio intermediario en servicios tradicionales, además en esta tecnología se asegura a la información de la cadena esté distribuida en todos los nodos, evitando que un nodo sea vulnerado o se pierda información. Cada bloque es agregado cronológicamente en la cadena con el acuerdo o consenso de la mayoría de todos los nodos.

Antes de que surja esta tecnología ya se venía usando el concepto de red de pares P2P (*peer to peer*), en programas de intercambio de archivos como Emule o Ares. La descentralización está basada en la confianza de conexiones entre pares marcando diferencia de las base de datos tradicionales porque no existe un ente central como servidor sino que tenemos una base de datos descentralizada, compartida y replicada.

Figura 1.2: Tipos de redes



Fuente: Sitio 101blockchains.com

Funcionamiento

El concepto de *blockchain* puede ser explicado a partir de cómo funciona internamente el *Bitcoin*, en el cual se producen intercambios de transacciones de activos.

El comercio de Internet está exclusivamente ligado a intermediarios como Instituciones Financieras que validan, aseguran y preservan las transacciones electrónicas debido a un cierto porcentaje de fraude y se requiere un ente mediador financiero y esto resulta en altos costos de transacción.

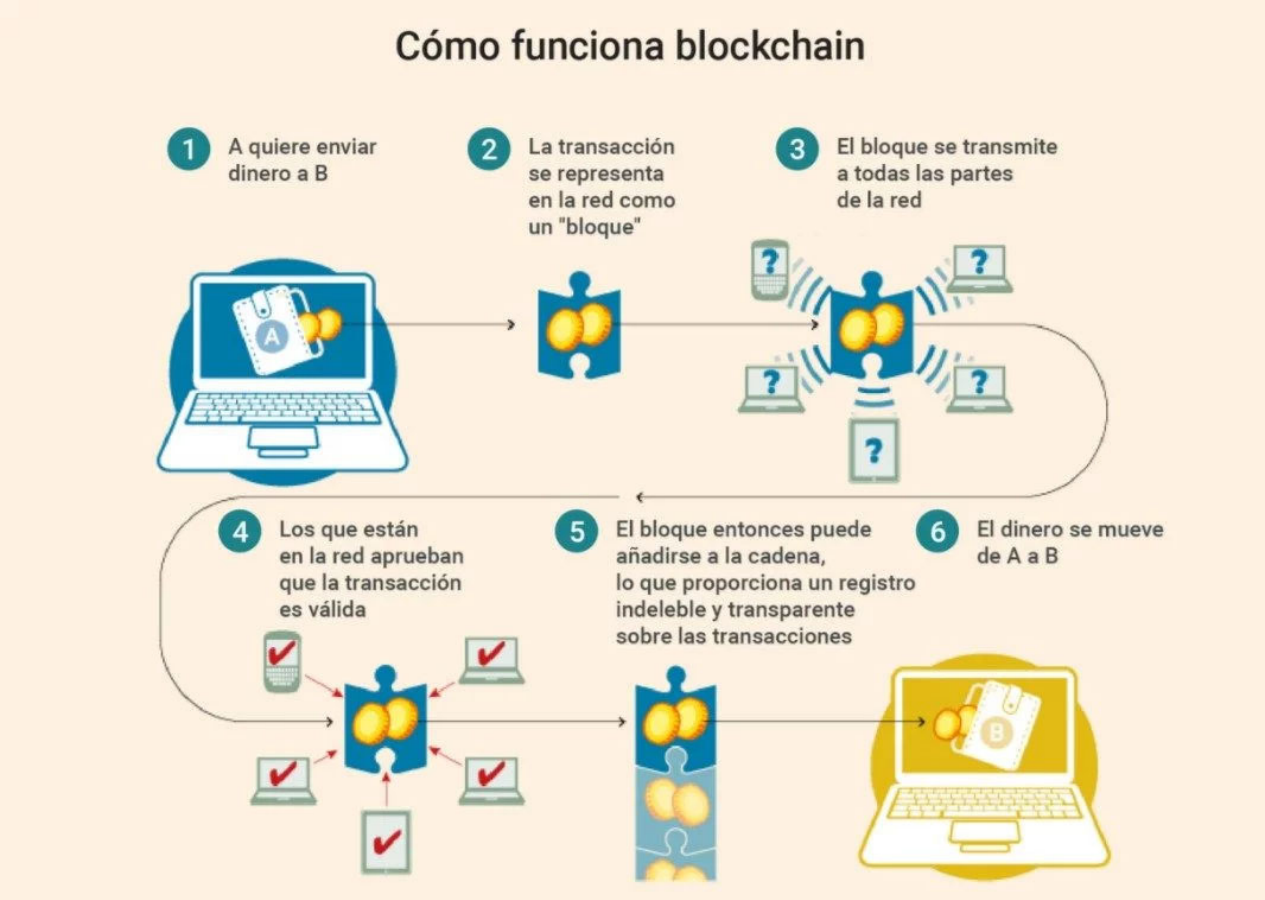
El *Bitcoin* no usa intermediario para realizar la transacción del activo porque se vale de la prueba criptográfica como seguridad del intercambio entre dos partes o usuarios disponibles en Internet usando la plataforma de *Blockchain*. El usuario que quiere realizar la transferencia de moneda digital tiene su propia clave privada para su cuenta pública para realizar el envio a otro usuario (este también tiene su propia clave privada a su respectiva cuenta pública) de la red *Bitcoin*.

La transacción (tal como se observa en la imagen Figura 1.3) es representada por un bloque, cuando un usuario A quiere enviar moneda digital a un usuario B, entonces el bloque es enviado a cada nodo de la red *Bitcoin* para verificar y validar la transacción , de darse válido por estos nodos ,se agrega el bloque transaccional a la cadena de bloques (también llamado libro público).

La validación en los nodos necesita garantizar dos cosas antes de agregar el bloque transaccional a la *Blockchain:*

1. El remitente posea su propia criptomoneda.
2. El remitente tiene suficiente criptomoneda en su cuenta.

Figura 1.3: Funcionamiento de *Blockchain*



Fuente: Sitio elpaisfinanciero.com/bitcoin

El orden de las transacciones se realiza agrupándolas en bloques tal que cada bloque sigue una cronología y todos los bloques están entrelazados por un *hash*(resultado de una función criptográfica), es decir un bloque tiene el *hash* del bloque anterior y así uno tras otro en toda la cadena. Pueden haber varias transacciones en un bloque y se consideran que ocurrieron en el mismo tiempo.

Para evitar las múltiples generaciones de bloques a la vez y no se sepa cuál es el próximo bloque para agregar. *Bitcoin* resuelve este problema introduciendo un protocolo de consenso, el cual consiste en agregar un bloque en la cadena, siempre y cuando contenga la respuesta especial a un problema matemático.

El protocolo de consenso es conocido como "*Proof of Work*"(Prueba de Trabajo) es decir cada nodo de la red va probando en forma iterativa hasta dar con la solución , el nodo que logre resolver el problema matemático tiene suficiente capacidad computacional y genera el bloque.

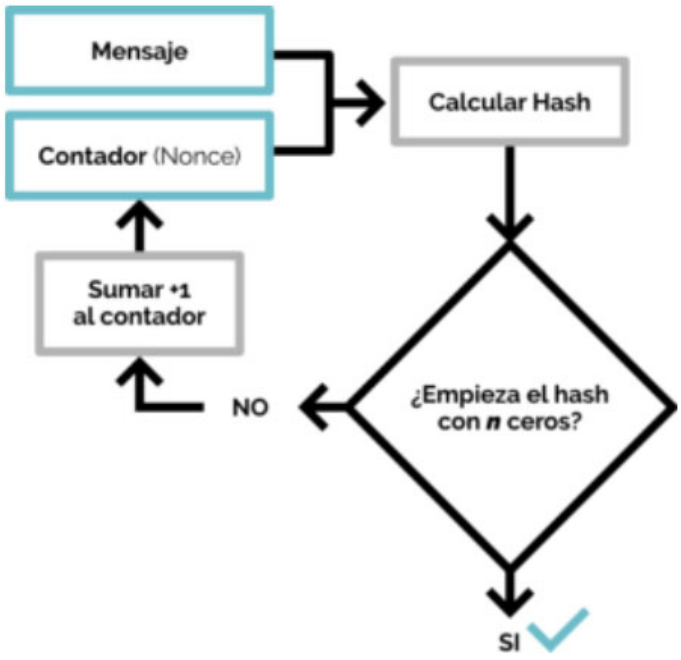
Cada nodo busca resolver el problema matemático hasta encontrar el "*nonce*", un número de 32 bits usado para encontrar el *hash* buscado (es la solución del problema matemático) y este contenga los ceros iniciales requeridos para agregar el bloque. Se requiere de gran esfuerzo de los nodos para encontrar la solución. El nodo que lo logre luego comunicará a los demás nodos de la red para que lo puedan verificar y así luego se agrega el bloque solución.

Proof of Work

La forma de generar el bloque, Satoshi Nakamoto incorpora un sistema del año 1997 llamado *hashcash* Figura 1.4, inventado por el criptógrafo inglés Adam Back. La idea era para evitar el *spam* de correo porque se sometía el mensaje de *mail* a una prueba de cumplir con la dificultad de generar un *hash* con ciertos ceros iniciales y para esto se usaba un número denominado *nonce* para ir cambiando las distintas salidas de *hash* hasta hallar el buscado y así enviar el correo.

Es así en *Bitcoin*, cada nodo compite con los demás nodos de la *Blockchain* para resolver un algoritmo complejo hasta encontrar la solución. Una vez logrado, el nodo ganador luego avisa a todos los nodos de la red para que verifiquen y así sea agregado el bloque correspondiente a la cadena comprobando que el nuevo bloque tenga el hash buscado. Este tipo de consenso es un método iterativo de búsqueda del valor del *hash* de la cabecera del bloque donde se usa el valor del *nonce* para obtener el resultado con la cantidad de ceros iniciales como requisito de la solución. El nodo ganador de esta competencia recibe una recompensa monetaria. Se requiere mucha capacidad computacional y mucha energía eléctrica en cada nodo. Este tipo de consenso es llamado Prueba de Trabajo o *Proof of Work*. Otra criptomoneda como *Ethereum* también usa este tipo de consenso.

Figura 1.4: Función *hascash*



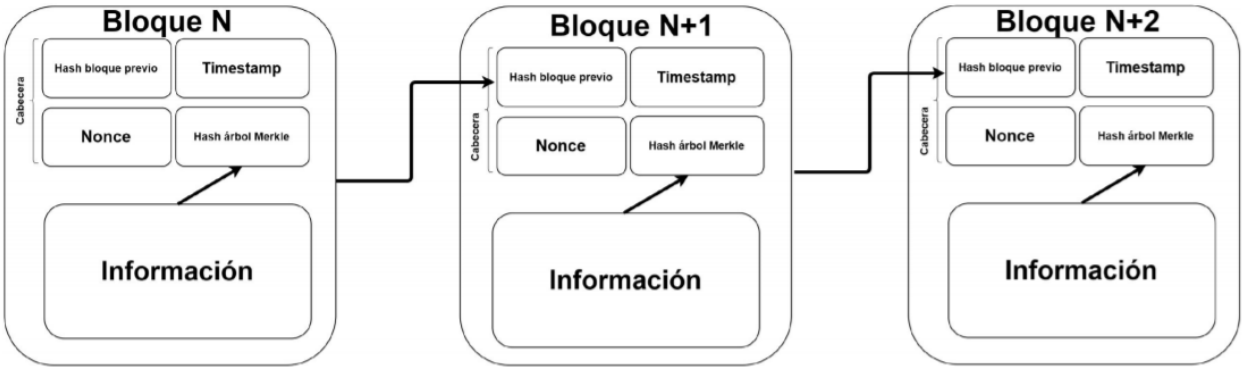
Esquema del proceso hashcash para encontrar una prueba de trabajo (hash) con dificultad n

Fuente: Alex Preukschat (2017)

Estructura de los bloques de la *Blockchain* de *Bitcoin*

Los bloques agregados a la cadena tienen la estructura como se muestra en la siguiente Figura 1.5 donde cada bloque tiene un *hash* del bloque anterior dentro de la cabecera y además el primer bloque de la cadena se lo denomina *Génesis.*

Figura 1.5: Cadena de Bloques



Fuente: Dolader, Bel y Muñoz (2017)

Tal como se muestra en la Figura anterior, cada bloque de la cadena del *Bitcoin* contiene la siguiente información:

•*Hash* bloque previo: El valor llamado *Hash* del bloque anterior permite a los bloques entrelazarse en forma secuencial formando la cadena.

• *Timestamp* (Marca de tiempo): Es una marca que identifica el tiempo o instante cuando se creó el bloque.

• *Nonce:* Es un contador secuencial que se usa por iteración por fuerza bruta en el proceso de minado hasta encontrar el *hash* solución.

• *Hash* árbol *Merkle*: Es un valor denominado raíz del árbol de *Merkle* de las transacciones,sirve como referencia para la consulta de toda la información contenida en el bloque. Con el valor raíz del árbol y otros valores adicionales se pueden hacer consultas de la información del bloque de manera segura y eficiente.

• Información: Son las listas de transacciones del bloque.

La información de los bloques en la red de *Bitcoin*, son las transacciones hechas con la criptomoneda, una de esas informaciones es la transacción correspondiente a la recompensa del creador del bloque por haber realizado el minado. En el 2009 la recompensa era de 50 *bitcoins* y luego después de 8 años llegó a 12,5 *bitcoins*. Se tiene previsto para años futuros se llegue a una emisión máxima límitada de 21000000 *bitcoins.*

Nodos Mineros

No es trivial la solución para generar el bloque y la complejidad del problema puede ser ajustado para que en promedio tome diez minutos a un nodo en la red *Bitcoin* resolver y generar el bloque. El primer nodo en encontrar la solución al problema luego avisa a los nodos restantes de la red.Los nodos consumen sus recursos computacionales para encontrar la solución. Estos generan los bloques y son llamados mineros donde se los premia con *bitcoins* por sus esfuerzos.

Criptografía

La criptografía realiza el cifrado de un mensaje o documento o archivo y como resultado se obtiene un mensaje ilegible de secuencia de caracteres de longitud fija. En *Bitcoin* se usa criptografía asimétrica ECDSA (Algoritmo de Firma Digital de Curva Elíptica) y *hashing* SHA-256(función *hash* criptográfica).

Para asegurar la información contenida en los bloques se aplica dos veces la función hash SHA-256 para dar integridad a las transacciones.

En cambio la criptografía asimétrica ECDSA es usada para generación de claves públicas a partir de las claves privadas. *Bitcoin* usa el algoritmo ECDSA, esta es una función del tipo elíptico y más eficiente a otro algoritmo como el RSA(*Rivest, Shamir y Adleman*). No es posible conocer la clave privada a partir de la clave pública con este algoritmo elíptico. No hay forma computacional o tecnológica actual para llegar a obtener las claves privadas a partir de las claves públicas en la *blockchain*. Además el ECDSA (*Elliptic Curve Digital Signature Algorithm*) es usado para firmar o verificar las transacciones.

Hash

La cadena de bloques son listas crecientes de registros de información cifradas donde cada bloque está encadenado al anterior con criptografía. Existe la función *hash* criptográfica, un algoritmo con ciertas propiedades para lograr el cifrado en la *blockchain*.

A la entrada de la función criptográfica, se toma un mensaje de cualquier tamaño y la salida será lo que se denomina *hash*, representado por una cadena alfanumérica única de longitud fija llamado también digesto, sin importar de que tamaño sea el mensaje de entrada en la función criptográfica.

El *Hash* es usado para verificar la pertenencia a una información de entrada, es decir si se cambia el mensaje original también cambia el *hash* o digesto de forma radical.

Un *hash* está representado por un código que se obtiene al procesar información a través de una función criptográfica, que si al modificarse esta información así sea un pequeño cambio ya sea esta una foto , cambios en el color o si es un texto ,un cambio en el acento , el *hash* va a cambiar totalmente.

Existen una variedad de algoritmos para la creación del *hash* en distintas plataformas para distintos usos como la autenticación de documentos, verificación de contraseñas, verificación de firmas digitales y en criptomonedas. Entre esta diversidad de funciones criptográficas están el *BLAKE2,MD6,Streebog* y el fundamental para *Bitcoin* es el SHA 256 (*Secure Hash Algorithm*).

La función SHA fue diseñada por la Agencia Nacional de Seguridad estadounidense (NSA) , previamente el diseño fue el SHA-1 y con el tiempo se fue mejorando el algoritmo al SHA-2.Luego de la familia SHA-2 viene el SHA-256 y es ampliamente usado por el criptomundo por ser el algoritmo escogido en el *Bitcoin* para hacer funcionar la *Blockchain* y luego se han derivado otras criptomonedas conservando el mismo algoritmo como es el caso de *Peercoin*.

Usando el algoritmo SHA256 en el siguiente ejemplo, se puede entender funcionamiento de la función *hash* con el mensaje de entrada:

Bitcoin es la primera criptomoneda

Y a la salida de la función criptográfica se obtiene el *hash*:

91D3081626672039C99F27323895D06B88376312706BF7AB035A662B6C5C0B1B

Y de cambiarse el mensaje de entrada ya sea añadiendo palabras, el *hash* cambiaria, por ejemplo si agregamos un punto al mensaje de entrada:

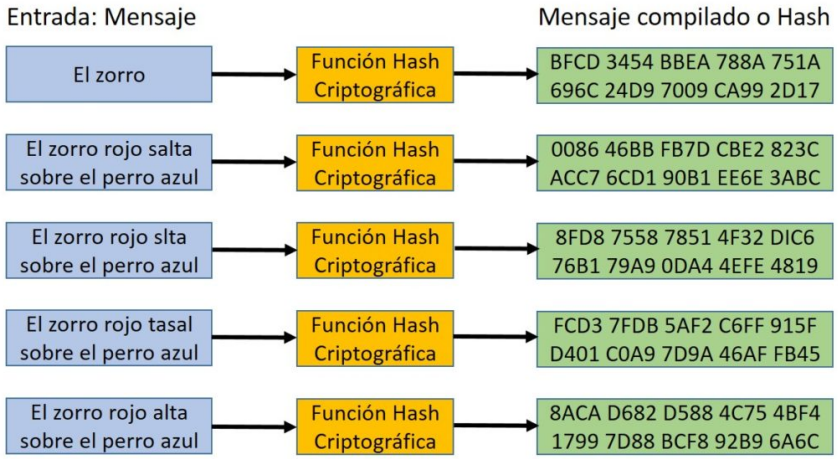
Bitcoin es la primera criptomoneda.

El *Hash* correspondiente es distinto:

AE0B40E7FC912BCE189A06F3A8069776FB24DCCC493332F2D349F0A470DE1254

Otros ejemplos del funcionamiento del *Hash* se pueden observar en la siguiente Figura 1.6:

Figura 1.6: Función de *Hash*



Fuente: Sitio criptonoticias.com y wikipedia

Así se transmiten los mensajes de forma segura e integra, donde es casi imposible de averiguar el mensaje original a partir del digesto o hash y por lo tanto tampoco sería posible modificarlos. Esto se conoce como funciones unidireccionales. *Bitcoin* usa el algoritmo SHA256 para generar el *hash* con un tamaño fijo de 256 *bits*.

Es por eso el uso de *hash* en el registro de documentos porque brinda la certeza que si alguien modifica el contenido, el *hash* sería totalmente diferente. De esta forma no hay necesidad de almacenar grandes archivos por ejemplo como fotos o videos en la *Blockchain,* se almacena solo el *hash*. Y los archivos por ejemplo como fotos o videos se guardan en la computadora, nube o servidor para que luego se pueda comprobar por si alguien modifica estos archivos.

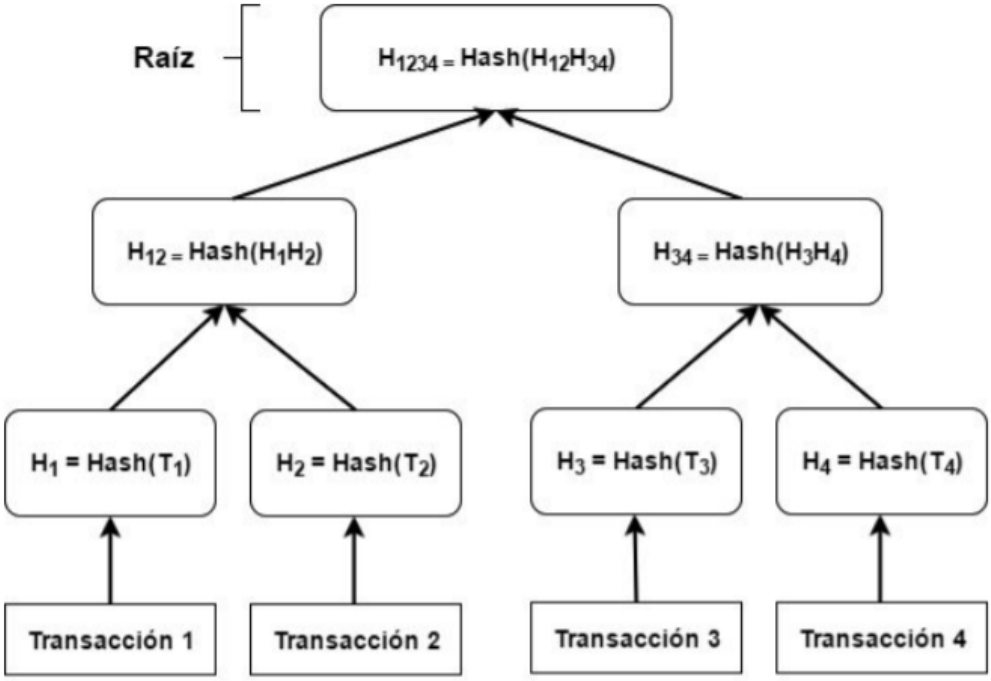
No se puede reconstruir la información original a partir del *hash*, de esa forma el hash publicado en la *Blockchain* es seguro porque ninguno pueda saber el archivo correspondiente al *hash*.

Árbol de Merkle

Las transacciones en la *Blockchain* usan *hashes* para el cifrado de datos y están ordenados mediante la estructura de Árbol de *Merkle* y se resumen a medida que crece la cadena, siendo así un método seguro , ligero y rápido para la verificación de datos.

El orden jerárquico del árbol es de arriba hacia abajo empezando por un único valor llamado raíz y luego se va dividiendo en nodos llamados hojas con valores de *hashes* que provienen de los datos de las transacciones. En la siguiente Figura 1.7 se puede observar el ordenamiento a partir de aplicar *hash* a cada transacción y como se resume hasta el nodo raíz:

Figura 1.7: Árbol de Merkle



Fuente: Dolader, Bel y Muñoz (2017)

El nombre de Árbol de Merkle proviene de su inventor Ralph Merkle, un científico computacional estadounidense que patentó la estructura del árbol en 1979, inventor también del *hash* criptográfico y de la criptografía de llave pública.

El propósito del árbol es crear la raíz de Merkle y es el valor que resume todos los valores de los nodos que están debajo de la estructura. En la *Blockchain* se resume a un solo punto llamado valor raíz de todos los *hashes* de las transacciones de un bloque. El resumen se crea juntando todos los hashes de las transacciones en pares y a su vez se va aplicando de nuevo la función criptográfica hasta llegar a la raíz. En un bloque existe una sola raíz de Merkle.

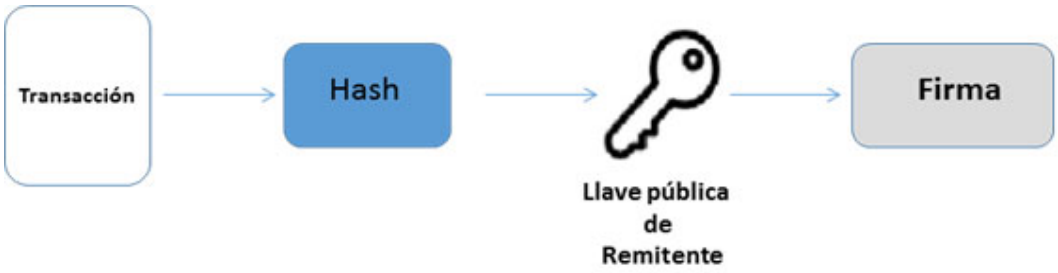
Por ejemplo si en un bloque hay 512 transacciones, con la estructura del árbol de Merkle se va ordenando en 256 pares, reduciéndose luego a 128, luego a 64 y así a 32,16,8,4,2 y llegando a resumirse en una sola línea alfanumérica que es un valor raíz y representa las 512 transacciones en lugar de que el bloque contenga 512 *hashes*. Usando el algoritmo SHA-256,cada hash pesa 32 bytes y siguiendo el ejemplo de 512 *hashes* el bloque tendría

que soportar más de 16384 *bytes* pero haciendo el uso de la raíz de Merkle solo se contiene 32 *bytes* en el bloque, conteniendo al resto de transacciones matemáticamente y no hay necesidad de incluir a todos.

Transacciones

El procedimiento de solicitud de transacción es el envio de *bitcoins* de un usuario a otro usuario mediante el uso de criptografía asimétrica. El usuario remitente para enviar *bitcoins* a la dirección del usuario receptor (este está asociado a una clave pública) usa la clave privada para firmar la transacción a realizar, obteniendo la firma electrónica. Y luego envia a la red *Blockchain* la transacción, la firma electrónica y la clave pública del remitente (Figura 1.8):

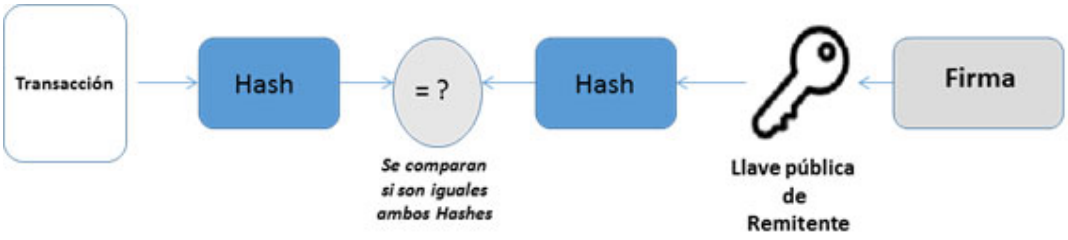
Figura 1.8: Proceso genérico de firmar el dato



Fuente: Adaptado de Alex Preukschat (2017)

La red *Blockchain* validará (Figura 1.9) la transacción enviada por el remitente, usando la clave pública del remitente para descifrar la firma y obtener el *Hash*. La red de nodos también aplica nuevamente el *Hash* a la transacción recibida por el remitente para comparar con el *Hash* obtenido en el proceso de descifrado anterior. De darse iguales los dos Hash, la firma es la correcta, si no es así, significa una transacción inválida.

Figura 1.9: Proceso de verificación de firma



Fuente: Adaptado de Alex Preukschat (2017)

De darse una transacción válida y de generarse el bloque, el usuario receptor puede ver su saldo de envio del remitente, usando su clave privada y así sabe la cantidad de *bitcoins* asociada a su clave pública o dirección pública.

1.2.2 Red *Ethereum*

Luego del *Bitcoin* , otra generación de red *Blockchain* de importancia aparece en el año 2014 de la mano de sus fundadores Vitalik Buterin , Gavin Wood y Jeffrey Wilcke , llamada *Ethereum* siendo una plataforma abierta donde se pueden construir y usar aplicaciones descentralizadas desplegadas sobre la tecnología *Blockchain.*

Ethereum se diferencia de *Bitcoin* porque es una *Blockchain* programable donde aparte de realizar transacciones de moneda virtual se cuenta con contratos inteligentes, estos son códigos programables y almacenados en la cadena de bloques para realizar las aplicaciones descentralizadas.

Los contratos inteligentes en *Ethereum* son acuerdos de dos o más partes interesadas, de modo de ejecución automática, ahorrándose tiempo y dinero en lo que costaría la intervención de terceros en el caso de un contrato tradicional.

Ethereum es una plataforma *Blockchain* distribuida y descentralizada. La moneda virtual en esta tecnología es el *ether* y para generar los bloques se usa el protocolo de consenso *Proof of Work* con el algoritmo llamado Dagger-Hashimoto (*Ethash*) con la función de *hash Keccak* (parecida a SHA).También existen otros métodos de consenso en otra versión de red *Ethereum.*

Los dispositivos usados por los nodos mineros en *Ethereum* usan la tecnología GPU (Unidad de Procesamiento Gráfico) siendo más flexible y de mayor capacidad para generar diferentes monedas virtuales a comparación de *Bitcoin* que usa la tecnología ASIC(Circuito Integrado para Aplicaciones Específicas) en los nodos mineros y son más dedicados a la generación de monedas virtuales específicas como el *bitcoin.*

La finalidad de *Ethereum* es tener otra red basada en *Blockchain* donde se desarrollen aplicaciones descentralizadas , donde cualquiera pueda encontrarse con esta plataforma abierta para crear un sistema descentralizado por ejemplo desplegar distintos casos de uso de *blockchain*, diferenciándose a la red *Bitcoin* nativa porque *Ethereum* está construida para que sea configurable, flexible y poder generar otras monedas virtuales.

Smart Contracts

En 1995 a través de Nick Szabo, jurista y criptógrafo mencionó en forma pública el concepto de contrato inteligente y dos años después en 1997 desarrolló un documento más detallado explicando los *Smart Contracts*. La mención y la explicación de estos contratos fueron en forma teórica y no se pudo en aquel momento llevar a la práctica porque no existía todavía la infraestructura hasta que entonces apareció *Blockchain* de *Ethereum* haciendo posible el uso práctico de estos contratos inteligentes.

Los contratos inteligentes almacenan el código ejecutable, datos y el balance denominado ether, estos contratos tienen también al igual que los usuarios una dirección, dando la posibilidad de realizar transferencias de contrato a nodos de la red o viceversa. También dentro un contrato se puede ejecutar funciones de otros contratos.

Ethereum es una *Blockchain* con lenguaje de programación de *Turing-Complete*, permitiendo flexibilidad en programar los contraltos inteligentes. La posibilidad de esta tecnología es desplegar una variedad aplicaciones financieras y no financieras.

Funcionamiento

El corazón del *Ethereum* es la Máquina Virtual *Ethereum*, este ejecuta distintos códigos de algoritmos complejos arbitrarios para realizar tareas complejas, por esto en términos de informática a *Ethereum* se lo denomina de *Turing* completo. Los desarrolladores pueden crear aplicaciones que corran en esta máquina usando lenguajes de programación amigables como *JavaScript* y *Python*.

El funcionamiento de la plataforma *Ethereum* se debe a que los nodos cuentan cada uno con una máquina virtual y ejecutan las mismas instrucciones de manera de mantener el consenso de la *Blockchain* con un protocolo de consenso de red *peer to peer* (de par a par) por eso a *Ethereum* se la describe como una computadora mundial.

Las Máquinas Virtuales de *Ethereum* ejecutan los *Smart Contracts* permitiendo interpretar su código programado. El lenguaje de programación de los *Smart Contracts* es el llamado *Solidity*.

En *Ethereum* se necesita del *token* para realizar transacciones y en el caso de una transacción con criptomoneda, el *token* es el *ether* y se almacena en una cuenta. Existiendo dos tipos de cuenta, una es la externa, propia del usuario y la otra es la cuenta de contrato inteligente. La cuenta externa es controlada por la clave privada del propietario o usuario y mantiene un valor de *ether* y puede ser usado para transacciones de transferencia de dinero o invocar a un *Smart Contract*. La cuenta de contrato es controlada por la lógica de código del contrato y tiene un cierto valor de *ether*.

1.2.3 Tipos de *Blockchain*

Desde la aparición de *Blockchain* con *Bitcoin*, esta tecnología fue evolucionando y captando el interés de distintos actores como gobierno, organizaciones y empresas, surgiendo diferentes tipos de redes:

Blockchain pública

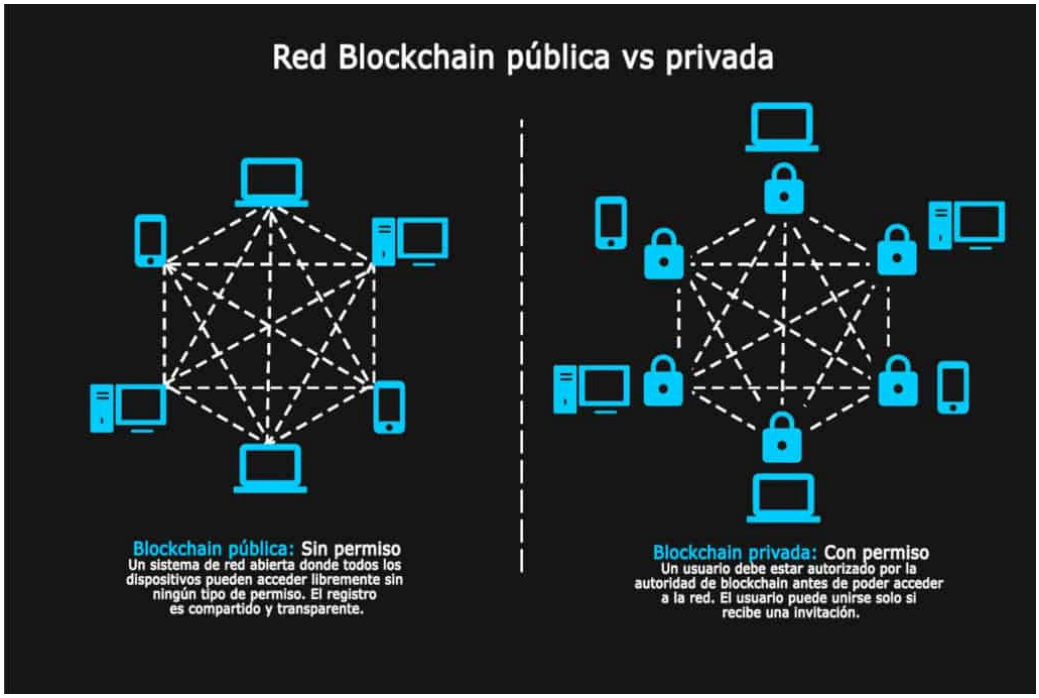
En este tipo de red cualquier nodo o usuario puede participar de la plataforma sin requisito de autorización de algún ente. Y el acceso al libro contable o a los bloques de transacciones es de forma pública, siendo una red transparente. Las plataformas de *Blockchain* de red pública son *Bitcoin, Ethereum* y entre otras. La aparición de variedad de estas plataformas públicas entre 2012 y 2015 estuvo de moda con distintas criptomonedas como *potcoin, healthcoin, peercoin, solarcoin o spaincoin.*

Blockchain privada

Para la participación en esta red se necesita la autorización de una entidad, corporación u organización. Las redes de este tipo son *Hiperledger, Corda y Quorum*. La aparición de estas plataformas se da entre el 2014 y 2015.

En la siguiente Figura se puede observar las diferencias:

Figura 1.10: Tipos de *Blockchain*



Fuente: Sitio 101blockchains.com

Blockchain Federada o Hibrida

La participación en una red hibrida se requiere autorización de partes como un subconjunto, es como una red privada contenida en una red pública. El acceso a las transacciones o registros es también limitado por la autorización de los administradores. Este tipo de plataformas es generalmente usado por sector gobierno y varias organizaciones que necesiten compartir información.

Cuadro 1. 1: Características de redes Blockchain

	Red Pública	Red Privada	Red Híbrida
Definición	Está abierta a todos, cualquiera puede participar.	Está controlada por los propietarios y el acceso está limitado a ciertos usuarios.	Es una combinación de la *blockchain* pública y privada. Esto significa que algunos procesos se mantienen privados y otros públicos
Transparencia	Es completamente transparente.	Es sólo transparente para los usuarios a los que se les otorga acceso.	La transparencia de la *blockchain* híbrida depende de cómo los propietarios establecen las reglas.
Incentivo	La *blockchain* pública incentiva a los participantes para hacer crecer la red.	La *blockchain* privada es limitada y, por lo tanto, no tiene un incentivo similar al de una *blockchain* pública.	La *blockchain* híbrida puede optar por incentivar a los usuarios si así lo desean.

Fuente: Adaptado del Sitio 101blockchain.com

Además del *Ethereum*, los contratos inteligentes pueden aplicarse también en otras *blockchain* privadas y públicas, tal como *Morax* y *Corda* , son plataformas en entornos privados o empresariales. En la *blockchain* pública de *Bitcoin* se agregan capas para sumar funcionalidades de la cadena de bloques para hacer apto el uso de contratos inteligentes, un ejemplo es la plataforma *RootStock* trabajando con *Bitcoin* y *Smart Contracts*.

1.2.4 Protocolos de consenso en *Blockchain*

Otras formas de generar y agregar el bloque a la cadena, está dado por los protocolos de consenso:

Prueba de Participación

En este protocolo no se requiere mucha capacidad computacional y no se hace demasiado gasto de energía a comparación de POW (*Proof of Work*), por lo que el método de consenso está dado por la cantidad de moneda digital de cada nodo y aquellos con mayor cantidad y además tengan más participación, tendrán más probabilidad de agregar bloques y validar transacciones. Los nodos mineros en este caso son llamados nodos validadores.

Se llega a tener más transacciones por segundo que en el caso de POW. La primera criptomoneda en hacer uso de este consenso fue *PeerCoin* en el año 2012, luego aparecieron proyectos como *Bitshares* y *NXT* usando Prueba de Autoridad(*Proof of Stake*).

Prueba de Autoridad

Los nodos validadores en este modo de consenso previamente para agregar bloques exponen su identidad real y reputación como garantía de transparencia. Este tipo de consenso hay un número limitado de validadores que cuidaran su reputación e identidad y serán escogidos por turno para agregar el bloque. No hay un tipo de recompensa en este tipo de protocolo, el gasto computacional y energético son menores que un POW. El consenso de Prueba de Autoridad (*Proof of Authority*) es usado en las redes *Kovan* y *Rinkeby* de *Ethereum*. Como así también hacen uso de este protocolo en *Hyperledger* y *Riple.*

Practical Byzantine Fault Tolerance

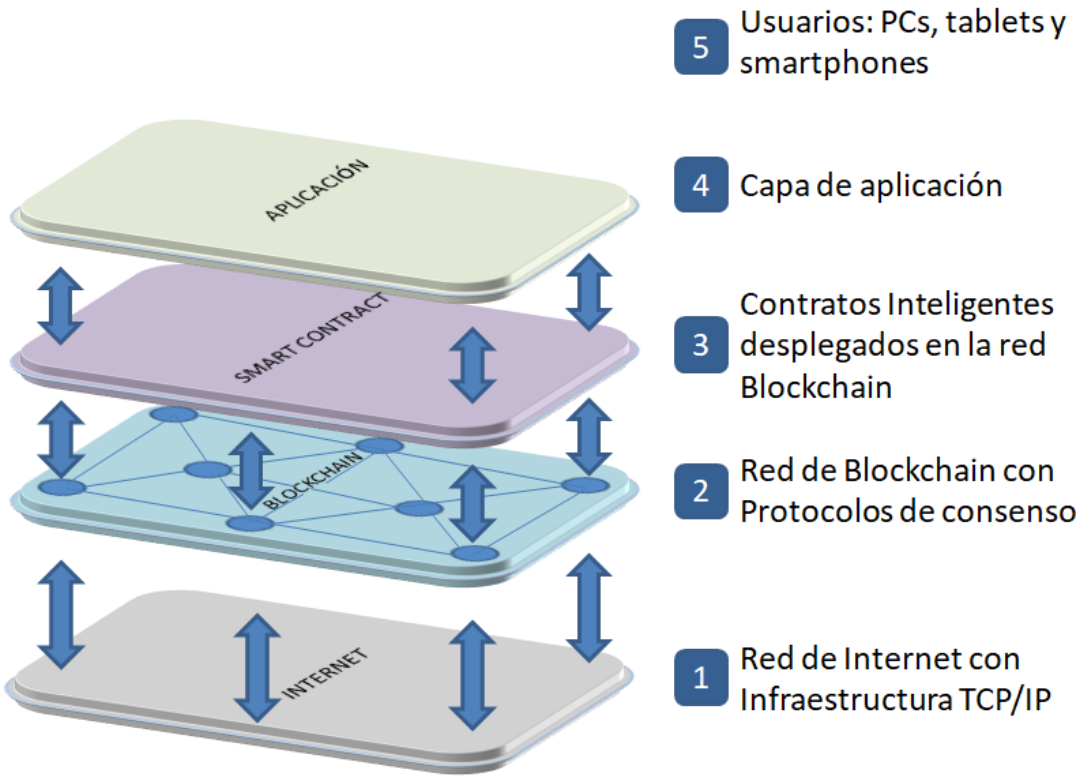
Es un algoritmo para alcanzar el consenso en la *Blockchain* y para aprobar las transacciones tolerando aquellos nodos maliciosos que fallan o brindan información errónea provocando errores.

1.2.5 Capas en *Blockchain*

Hasta ahora se fue avanzando en la mención del inicio del Internet de la Información hasta llegar al concepto del Internet del Valor con la aparición de las criptomonedas. Y en estas monedas virtuales está la base tecnología *Blockchain* y su evolución en muchas plataformas públicas, privadas e híbridas.

En la siguiente Figura 1.11 se representa un resumen de cómo se va agregando en capas a la base de Internet. En capas superiores se ven la base tecnológica de *Blockchain* , *Smart Contract*, Aplicación y la Interfaz a usuario:

Figura 1.11: Aplicación , *Smart Contract*, *Blockchain* e Internet



Fuente: Adaptado de 101blockchains.com

Los elementos claves para el funcionamiento de *Blockchain* son la criptografía, el consenso y la cadena de bloques. La criptografía asegura la información de registro en la cadena de bloques vinculado con el consenso de todos los nodos de la red para guardar las transacciones validadas.

1.2.6 Blockchain Federal Argentina

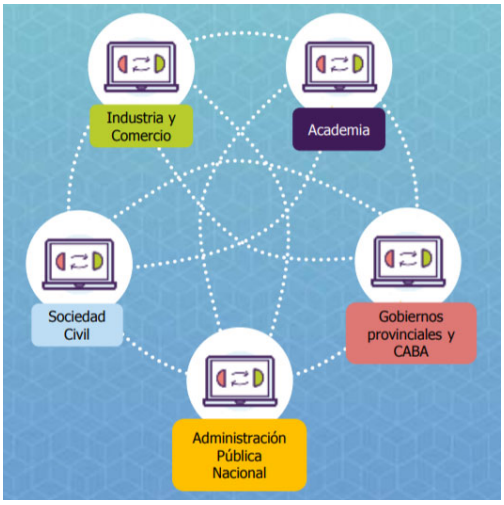
En el 2018 en Argentina con las iniciativas de las tres organizaciones Ariu, CABASE y NICar dan inicio a la primera *Blockchain* federal en el país con la idea de que se vuelquen servicios y aplicaciones en una plataforma de innovación tecnológica segura, confiable y transparente. El proyecto nace como un trabajo colaborativo y apunta a seguir ese camino con un modelo de trabajo de múltiples partes interesadas conformando así la Blockchain Federal Argentina (BFA), optando por una estrategia donde todos los que participan es esencial, desde la Infraestructura hasta la Ingeniería Organizacional.

Figura 1.12: Logo de *Blockchain* Federal Argentina

Fuente: Documentos Introductorios *Brief* BFA

Las múltiples partes interesadas en BFA están representadas por distintos sectores como Industria y Comercio, Académico, Gobierno Nacional, Gobierno Provincial y CABA y Sociedad Civil.

Figura 1.13: Participación sectorial



Fuente: Documentos Introductorios *Brief* BFA

La infraestructura principal son los nodos selladores (similar a los nodos mineros), estos agregarán bloques a la cadena. En el 2018 se fueron sumando 23 nodos selladores desde que inició a operar la plataforma, hoy en día están en vía de sumar más nodos miembros como selladores.

También existen otros tipos de nodos para ayudar a las conexiones de nodos selladores y se establezca comunicación entre ellos, estos son conocidos como nodos *gateway* y *bootnode*.

Otros nodos pertenecientes a BFA son los transaccionales donde operan las aplicaciones y por otro lado están los nodos de lectura, estos solo pueden observar el funcionamiento de la red de cómo se van generando los bloques pero no pueden intervenir en el agregado de bloques en la cadena.

La tecnología de base de BFA es la de *Ethereum* siendo esta una de las *blockchain* públicas más difundidas a nivel internacional y fue conocida en su inicio con el protocolo de consenso de Prueba de Trabajo. Pero *Ethereum* es una plataforma flexible y programable, su desarrollo es basado en código abierto para toda la comunidad y se puede adaptar a otros contextos y necesidades como optar por otros protocolos de consenso.

BFA toma el *software* de *Ethereum* adaptando a la necesidad de un modelo liviano usando el tipo de consenso de Prueba de Autoridad sin uso de criptomonedas.

El *software* implementado en BFA es abierto y robusto al igual que los desarrollos y modificaciones realizados serán abiertos a cualquier interesado, consolidándose en una plataforma como herramienta colaborativa.

El modelo elegido es liviano porque no está pensado para transacciones de criptomoneda, no se hace gasto en energía y capacidad computacional, ser parte de la red tiene un costo marginal. Las transacciones son sin costo pero para operar transacciones, cada nodo tendrá a disposición del *ether* asignado mediante una destilería (esta es programada en un Contrato Inteligente) que asignará el *ether* suficiente y en forma periódica a cada nodo.

El almacenamiento en BFA serán solo *Hashes* de archivos o documentos, evitándose cargar la red, solo queda el digesto en la *Blockchain* como registro correspondiente a una fecha y tiempo .La responsabilidad de los archivos usados para registro es parte del usuario de la red.

La Prefectura Naval Argentina fue uno de los primeros nodos selladores en sumarse a la BFA como una Organización Publica, de esta forma agrega a su plataforma de Internet la tecnología de *Blockchain* con el propósito de optimizar los procesos de registros y abre a un mundo de aplicaciones en el futuro. La institución es parte de esta innovación tecnológica porque cuenta con características de seguridad, transparencia e integridad. Y da lugar a un caso de uso que es parte de la implementación de este trabajo.

En la siguiente Figura 1.14 se observan los distintos organismos siendo parte de la red de nodos selladores de BFA.

Figura 1.14: Partes miembros de BFA

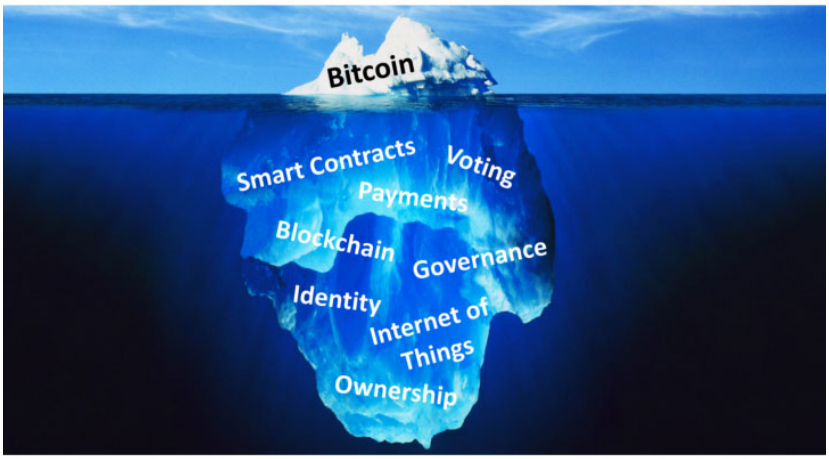
Fuente: Documentos Introductorios *Brief* BFA

Anexos de artículos y eventos de la importancia de los *stakeholders* sobre *Blockchain*.

Capítulo 2. Casos de uso

Los primeros casos de usos fueron enfocados en el sector económico y donde más se vino desarrollando con la aparición de las criptomonedas. La mayoría de los expertos afirman que el *bitcoin* es solo la punta del iceberg del potencial de aplicaciones con tecnología *Blockchain.*

Figura 2.1: Aplicaciones de *Blockchain*

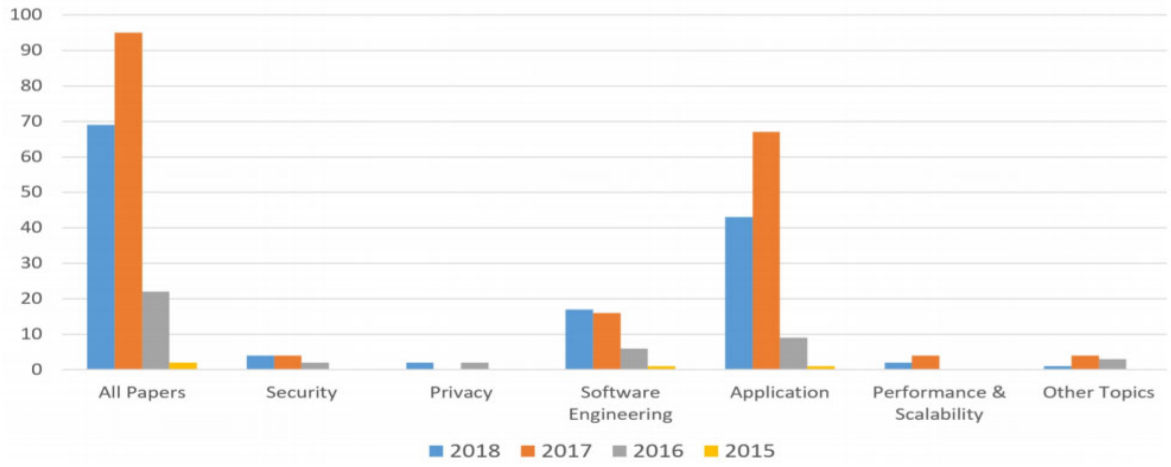


Fuente: Sitio nestoraltuve.com

2.1 Importancia de los *Smart Contracts*

Desde la aparición de los Contratos Inteligentes con *Ethereum*, hubo un incremento en el interés académico de investigación aumentando año tras año la publicación de *papers* relacionados con *Smart Contracts.* Tal como se puede observar en la siguiente Figura 2.2 que desde el año 2015 hasta el año 2018 los tópicos de importancia sobre Contratos Inteligentes fueron Seguridad, Privacidad, Ingeniería de *Software*, Aplicaciones, Performance y Escalabilidad y entre otros.

Figura 2.2: Temas de publicación sobre *Smart Contracts*

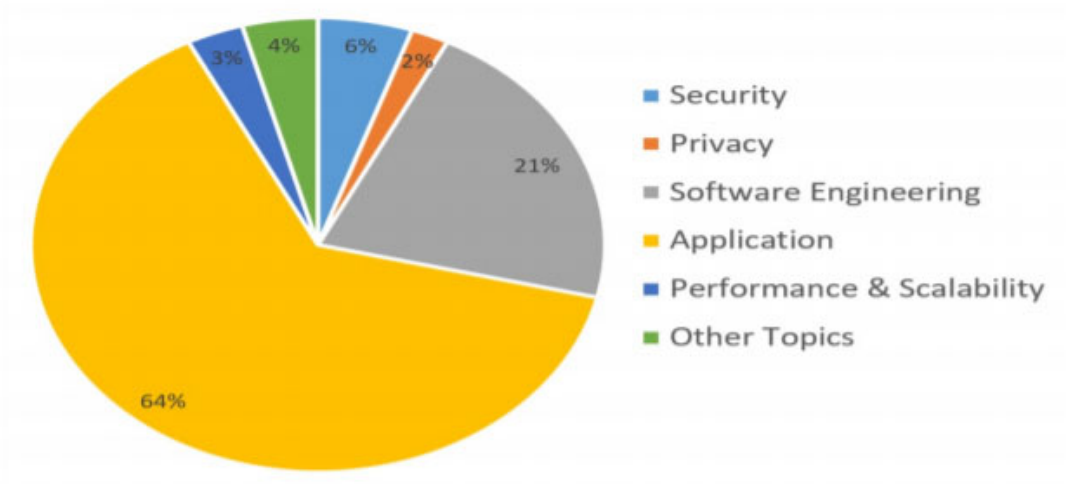


Fuente: Alharby,M.; Aldweesh,A. y Moorsel, A.(2018)

El tópico de mayor interés en publicaciones de *papers* es el uso de *Smart Contracts* para Aplicaciones en *Blockchain*.

La siguiente Figura 2.3 muestra el tópico más relevante en porcentaje con 64% y es el de Aplicaciones con *Smart Contracts* con mayor publicación en *papers* en comparación a otros tópicos.

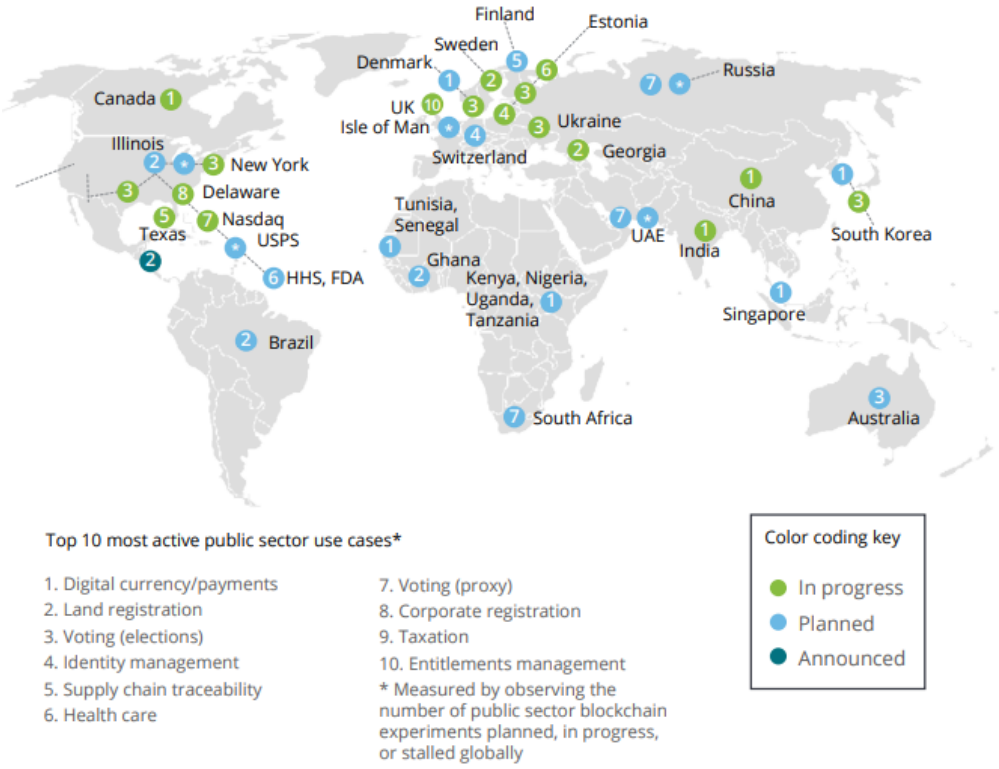
Figura 2.3: Tópicos de mayor relevancia con *Smart Contract*



Fuente: Alharby,M.; Aldweesh,A. y Moorsel, A.(2018)

También existe una publicación de *Deloitte University* informando mediante un artículo del uso de *Blockchain* en el sector público, involucrando varios países en exploración de pruebas de caso de usos. Donde se rescata el interés del valor agregado de Blockchain en registros de tierras, sistemas de votación y la identidad digital.En la siguiente Figura 2.4 correspondiente al informe de *Deloitte University* ,se puede observar los casos de uso en el sector público a nivel mundial.

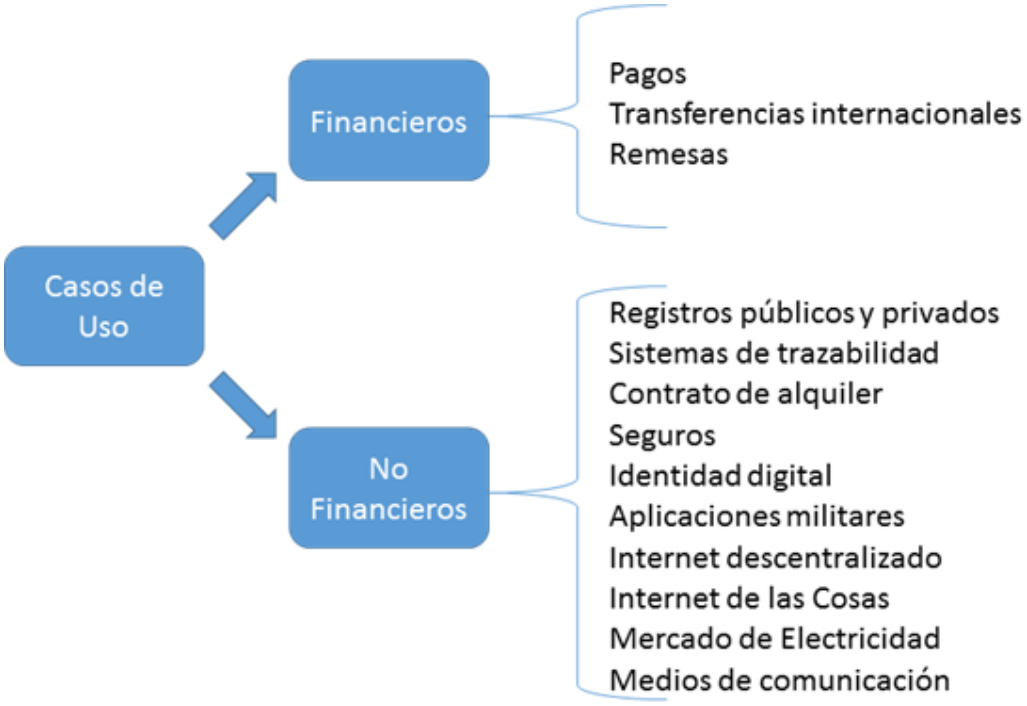
Figura 2.4: Casos de uso en el sector público a nivel mundial



Fuente: Análisis de *Deloitte* en conjunto con la *Fletcher School en Tufts University* (2017)

Dada la importancia remarcada de aplicaciones en los *papers* de los *Smart Contracts* y como se viene desarrollando *Blockchain* en distintos ámbitos, los casos de uso se pueden clasificar en Financieros y no Financieros, Figura 2.5:

Figura 2.5: Casos de uso



Fuente: Elaboración propia

2.2 Casos de uso Financieros

Las *blockchain* públicas como *Bitcoin* y *Ethereum* son preferidas por las *Fintechs* porque acaparan a cualquier usuario que no tenga una cuenta bancaria y de esta forma se logra ofrecer servicios a personas o entidades, para pagos, transferencias internacionales y remesas. Como ejemplos de empresas usando cadena de bloques están:

• *Abra* (goabra.com): con un servicio de remesas persona a persona.

• *BitPesa* (bitpesa.com): con envíos de dinero a y desde África, en países como Kenia, Nigeria, Tanzania y Uganda. Permitiendo a un pequeño comerciante pueda desarrollar su negocio de importación y/o exportación a una mayor agilidad y un menor costo en el envío de dinero.

• *Circle* (circle.com): es una *startup* para envíos de dinero sin comisiones, usando criptomonedas con destino a países desbancarizados o con control de divisas.

En cambio las *blockchain* privadas como por ejemplo *Ripple*, son preferidas por los bancos y entidades financieras por un motivo de hacer más confidencial la información compartida en el registro de transacciones y un uso especializado son los pagos internacionales interbancarios.

También el uso de la cadena de bloques reduce costos operativos y tiempos en servicios tradicionales de la banca. Otras plataformas de *blockchain* privadas son *Hyperledger* y R3.

Es decir las ventajas de usar la cadena de bloques en la banca, están en la automatización del proceso porque se elimina intermediarios y comprobaciones manuales, logrando una reducción notable de costos. También se logra reducir los tiempos en las transferencias, incluso las internacionales se resolverían en minutos. Un ejemplo es el Banco Santander que aplica *Blockchain* para transferencias internacionales ultrarrápidas.

También se ha usado *Blockchain* en donaciones con criptomonedas como el tercer sector de las ONG, *Save the Children* y *United Way* , estas organizaciones aceptaron monedas virtuales como forma de financiación

En un momento existió una aplicación llamada *ChangeTip* para dispositivos móviles con conexión a Internet, donde se podía realizar microdonaciones desde cualquier lugar y cualquier hora.

Actualmente *BitGive* es una ONG especializada en *bitcoins* y cuenta con una plataforma pública *GiveTrack* creada para la canalización de donaciones transparentes y financiar proyectos. Es uno de los proyectos más destacados como ONG.

El uso de Contratos Inteligentes con *blockchain* puede usarse en cheques digitales, venta de acciones virtuales,pagarés e Instrumentos financieros.

2.3 Casos de uso No Financieros

Más allá del *Bitcoin* y otras criptomonedas, existen muchos casos de usos no financieros que se pueden clasificar como:

Cuadro 2.1: Casos de uso No Financieros

Registración y Verificación	Trazabilidad	Contratos	Descentralización	Gestión de Identidades
Registros médicos	Ingredientes alimenticios	Seguros	Internet de las cosas	Identidad Digital de Personas
Registros de propiedad	Obras de arte	Seguridad automática	Internet	Identidad Digital de Organizaciones
Registro de vehículos	Diamante	Alquiler	Sistema de votación	Identidad Digital de Dispositivos
Registro de Propiedad Intelectual	Agricultura	Medios de comunicación		
Documentos	Donaciones	Licencias de música		
Aplicaciones militares		Mercado de Electricidad		
Servicios de notaría				

Fuente: Elaboración propia

2.3.1 Registro y verificación

Dada las características de *Blockchain* como registro inmutable de las transacciones, se puede usar esta tecnología para el almacenamiento de todo tipo de información obteniendo así un registro distribuido, inalterable, más seguro que las bases de datos centralizadas gestionadas por un intermediario.

Existen empresas que ofrecen estos servicios de registros descentralizados como *Tieron*, *Factom* y *Proof Existence* de *Bitcoin.*

Casos más específicos con gran posibilidad en el sector público y empresarial son:

- En clínicas y hospitales para la creación de un registro de datos y el historial médico de los pacientes.

- En el registro de propiedad para que figure quien es el propietario de cada terreno, inmueble y todas las transacciones de compraventa que se realicen, evitando fraude y manipulación.

- En el registro de vehículos.

- En la protección de la propiedad intelectual y la creación de productos digitales creativos de música, fotos, libros electrónicos y entre otros. Se puede cifrar una obra original y este cifrado registrarlo en la *blockchain* quedando así almacenado como una transacción con una autoría y fecha de registro. *Proof of existence* (Prueba de Existencia) de *Bitcoin* ofrece este servicio.

- En el registro de nacimientos, defunciones, matrimonios y divorcios.

- En registro de antecedentes penales internacional.

- Almacenamiento de un registro de todas las conversaciones de *Slack* de una empresa.

- **República de Giorgia :** En asociación con *Bitfury* desarrolló títulos de propiedad con tecnología *blockchain* para la Agencia Nacional de Registro Público del país.

- **Estonia :** Primer país en usar *blockchain* a nivel nacional, como uno de los países más adelantados en temas tecnológicos en su administración estuvo trabajando con *Bitnation* para que los residentes con identidad digital registren sus uniones matrimoniales y partidas de nacimientos en *blockchain.*

Luego de que Estonia tuvo la experiencia con los ciberataques de 2007, el país desarrolló la tecnología de bloques para garantizar la integridad de los datos ,almacenando estos en repositorios gubernamentales y así proteger sus datos contra amenazas.

Estonia se convirtió en sede del Centro de Excelencia Cooperativa de Defensa Cibernética de la OTAN y de la agencia europea de IT.

Este país báltico hace uso de la cadena de bloques en sus registros empresariales y fiscales, extendiéndose también a registros sanitarios electrónicos de sus ciudadanos.

- **Japón :** Usará *Blockchain* para el registro de propiedad y bienes raíces.

- **Suecia :** Junto a la compañía *ChromaWay* llevó con éxito la en prueba de registros de propiedad y bienes raíces usando *Blockchain.*

- **India :** El gobierno de Andhra Pradesh se ha asociado con *ChromaWay* para construir un sistema basado en Blockchain para el registro de tierras.

- **Honduras:** La empresa *Factom* estuvo en colaboración con el gobierno de Honduras en el desarrollo de un programa para la gestión del registro de la propiedad de la tierra con tecnología *Blockchain.*

- **Australia:** Se investigó el uso de *Blockchain* en seguridad de comunicaciones gubernamentales. También en seguridad pública donde el Gobierno estableció que los videos filmados pertenecientes a la policía sean almacenados en la cadena de bloques para garantizar su integridad. Otro caso de estudio del Gobierno federal australiano es la monitorización de los fondos públicos destinados a gobiernos locales. Y el otro campo de estudio es la seguridad alimentaria.

- **Singapur:** El Gobierno desarrolló con los bancos locales un sistema de *Blockchain* para combatir fraudes en las relaciones entre comerciantes y bancos. Antes los

defraudadores usaban facturas duplicadas para la obtención indebida de dinero de los bancos. Usando un *hash* para la factura se evita el fraude.

- **Dubái:** El Gobierno tiene previsto el traslado de documentos a una cadena de bloques y no emplear papel. Además identificó seis proyectos piloto en *Blockchain* para registros de transferencias de títulos, registros de salud, comercio de diamantes, registro de empresas, impulso del turismo y testamentos digitales.

- **Ghana y Rusia:** Exploraron también proyectos con *Blockchain* en registros de títulos de propiedad.

Servicios de notaría

Uso de notaría de forma fácil y barato con la verificación de la autenticidad de todo tipo de documento registrado en la *Blockchain* eliminando la necesidad de que un tercero lo certifique.

Compañías como *Stampery* y *Blockverify* usan *Blockchain* de *Bitcoin* para la verificación de correos electrónicos, documentos y productos farmacéuticos.

El servicio de certificación de documentos brinda confianza de la autoría de quien lo ha creado, de su existencia del momento (tiempo y fecha) y de la integridad de que no haya sido manipulado.

Los servicios son legalmente vinculantes porque la *Blockchain* no es manipulable y es transparente, permitiendo la verificación por terceros independientes.

Las ventajas de usar *Blockchain* en servicios de notaría son:

- Se tiene más seguridad, no se necesita de un tercero o un intermediario en la certificación de un documento evitando de que una persona pueda corromper. En cambio la tecnología *Blockchain* no puede ser alterada.

- Es muy barato, no hace falta la necesidad de contar con intermediarios como lo es en los casos de notaría tradicional.

- Se puede registrar todo tipo de documentos de forma anónima, *Blockchain* garantiza la privacidad de lo registrado.

- La compañía *Uproov* usa *Blockchain* en sus servicios de notaría donde se pueden registrar creaciones multimedia hechas desde un *Smartphone*, especialmente para ocasiones donde se quiera demostrar que hubo una reunión o evento concreto en un lugar con fecha y hora y con la documentación correspondiente a esa ocasión no fue alterada.

Existen otras compañías ofreciendo Gestión de derechos de propiedad intelectual:

- La compañía *Ascribe* está certificando la autoría usando *Blockchain* y además brinda un servicio de transferencia de propiedad con la mención al autor original.

- Empresas como *Mediachain.io* y *CoalaIP.org* están intentando crear nuevos protocolos descentralizados para etiquetar contenidos digitales en bases de datos descentralizadas. Y en un futuro estas bases sean registros universales para licencias de contenidos digitales. Se podría hacer uso también de aplicaciones y servicios con estos protocolos descentralizados para los creadores de contenido y estos puedan etiquetar, almacenar y distribuir sus creaciones. Es una manera de control para los artistas sobre su obra y hagan su rastreo si es usado por otro artista y así recibir compensación monetaria.

- Otras empresas como *Monegraph*, *Verisat* y *Blockchai*, están dedicándose al registro, en base a *Blockchain* para la propiedad intelectual

Aplicaciones Militares

El Ministerio de Defensa estadounidense y la OTAN ya pusieron en marcha proyectos relacionados con la tecnología *Blockchain* en el Ejército.

La Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) del Ministerio de Defensa estadounidense quiere aprovechar el uso de *Blockchain* en la creación de un servicio de mensajería seguro como propuesta titulada *Secure Messaging Plataform* y que está registrada como parte del Programa SBIR (*Small Business Innovation Research Program*) con el objetivo de desarrollar la plataforma, permitiendo transferir mensajes mediante un protocolo de seguridad descentralizado.

Por el lado de la OTAN evaluó propuestas del 2016 *Innovation Challenge* donde había un apartado titulado como Aplicaciones militares de las *Blockchains.*

2.3.2 Trazabilidad

Se puede usar *Blockchain* para hacer un seguimiento completo de cada parte de un producto procedente de lugares diferentes hasta su llegada a la compañía donde se lo ensambla o elabora y comercializa el producto final.

Existen compañías haciendo uso de *Blockchain* como son *Provenance.Org*, *SkuChain* y *Everledger* para la cadena de suministros realizando el seguimiento y garantizando la procedencia de distintos productos desde ingredientes alimenticios, productos de agricultura, diamantes a obras de arte. *Blockchain* brinda una solución a las falsificaciones y facilita la trazabilidad de productos y puede otorgar una certificación por ejemplo de que el producto es ecológico.

ONG

La aplicación de *Blockchain* al tercer sector como las ONG en ayuda humanitaria permite la trazabilidad de todas las acciones que suceden desde la instancia de la donación hasta que esta llegue al objetivo y genere impacto social, traduciéndose en una mayor transparencia.

Existe la *startup ComGo*, una herramienta para la trazabilidad de las donaciones, permite ver quienes son los donantes de cada actividad, el material comprado validado mediante una foto o una factura, en fin ver los hitos de un programa concreto de ayuda.

Las ONGs mencionadas para las pruebas piloto de *ComGO* son *Homeless Entrepreneur*, *It-willbe.org*, Fundación *Recover*, *KUBUKA*, Farmacéuticos sin Fronteras, Fundación *Exit*, Orden de Malta y Cáritas.

2.3.3 Contratos

Seguridad automatizada

Usando Internet de las Cosas, Identidades Digitales y contratos inteligentes , todo esto combinado en *Blockchain*, permitirá tener aplicaciones de sistemas de seguridad automatizados como por ejemplo aplicados a cerraduras automáticas (y estas conectadas a internet) que van a garantizar o impedir el acceso de personas (registradas a *Blockchain* con identidad digital) por ejemplo a un coche, casa o sala de una compañía.

Alquiler de propiedades y economía colaborativa

Se puede hacer un contrato inteligente de alquiler, por ejemplo de un propietario que quiera alquilar un piso o vehículo lo podría hacer mediante un *Smart Contract* desplegado en la *Blockchain* donde el propietario fije un precio por un tiempo dado. Siendo así aquella persona que quiera alquilar, realiza un pago con una transacción registrada en la *blockchain*, el contrato inteligente permite el acceso a la propiedad que le alquila el propietario por un tiempo concreto establecido. Existe la compañía *Slock* ofreciendo este servicio.

En el caso de uso de economía colaborativa existe la aplicación *La'Zooz* que ofrece el servicio mediante la compartición de coches basada en tecnología *Blockchain*. Siendo más barato el costo del servicio de usar un auto contratando en forma directa con la persona dueña del automóvil sin la existencia de intermediarios.

Contratos automáticos con IoT

El *Smart Contract* de *Ethereum*, es un código que se programa con ciertas condiciones en

términos de contrato entre partes y se almacenan en la *Blockchain*, los contratos inteligentes son autoejecutables evitando de esta manera a los intermediarios, disminuyendo costos y agilizando el cumplimiento de lo acordado en ese código programable. Se puede hacer uso de los *Smart Contracts* junto a la tecnología del Internet de las cosas (*IoT*) en:

- En una compraventa, usando un GPS(Sistema de Posicionamiento Global) para monitorear la venta, donde el contrato inteligente envie el pago al proveedor y al transportista en cuanto el paquete sea entregado a destino del cliente.

- En el contrato inteligente para el alquiler de vehículo, en caso de impago por parte del que alquila, se le impida encender el vehículo.

Licencias de música

Desplegar un Contrato Inteligente en la *Blockchain* para licencias de uso de música pertenecientes de otros artistas y entonces se pueda hacer los pagos correspondientes a los autores sin necesidad de intermediarios, logrando a que reciban más dinero por sus trabajos.

Mercado de electricidad

Usar sistemas de energías renovables es menos el costo que depender de un proveedor central de energía para abastecer la casa, empresa o edificio público. Además si se aplica *Blockchain* en una red distribuida donde se conectan casas y edificios, estos como usuarios podrían comprar energía o vender los excedentes a través de contratos, dependiendo de la necesidad en cada momento sin la existencia de una autoridad central para el control. Los pagos y los intercambios de energía se corresponden con transacciones que se almacenarían en la *Blockchain* permitiendo la verificación de cada transacción por los miembros de la red.

Blockchain impulsa la implantación de un nuevo modelo de sistema eléctrico, la compañía *Siemenes* apuesta a proyectos de *blockchain* en generación distribuida y ha invertido en la

compañía *LO3*. Y junto a otra empresa *ConsenSys* desarrollaron en *Brooklyn (USA)* las pruebas de las ventajas de un sistema descentralizado en *Blockchain.*

La compañía eléctrica *Vattenfall* ha realizado experimentos de *Blockchain* en compraventa de energía punto a punto, esto a través de una plataforma llamada *Powerpeers*.

La compañía *Power Ledger* con *Blockchain* experimentó almacenar baterías con el excedente de energía renovable. Y luego usar la batería cuando no se cuente con la energía renovable o también venderla al mercado eléctrico.

También la empresa eléctrica *RWE* junto a otra empresa llamada *Slock.it* habían lanzado el proyecto para gestionar la carga de coches eléctricos mediante los Contratos Inteligentes en *Ethereum*.

Sector de medios de comunicación

En lugar de pagar suscripciones mensuales o anuales en el acceso de sitios web o periódico digital con un costo elevado, se podría usar *Blockchain* , cobrando a los lectores por página o artículo para el acceso de los contenidos seleccionados por el lector cuando realice el pago correspondiente y así quede registrado el pago en la cadena de bloques.

Sector seguros

Se usaría *Blockchain* combinando los contratos inteligentes y el Internet de las Cosas , revolucionando el sector de los seguros y brindando a los usuarios un sistema de gestión con demandas más transparentes. Es decir , por ejemplo hogares y vehículos que estén con dispositivos y sensores conectados al Internet de las Cosas, se puedan detectar automáticamente incidentes y evaluado el daño, realizar el pago correspondiente al afectado, correspondiéndose con las condiciones del seguro plasmado en el contrato inteligente sin la necesidad de solicitar en forma expresa el pago de daños.

Existe una plataforma llamada *Blockchain Insurance Industry Initiative-B3i* , un consorcio donde lo integran *Aegon, Allianz, Munich Re, Swiss Re y Zurich.* Esta plataforma es para probar y explorar casos de uso con *Blockchain.*

Seguro en la salud

Las aseguradoras de salud con la aplicación de *Blockchain* junto a *Smart Contracts* podrán disminuir los costos administrativos. Y además se podrá relacionar automáticamente y de forma descentralizada los datos de acuerdos, transacciones y registros médicos, facilitando la comunicación entre asegurados, médicos y empresas aseguradoras. La ventaja de un contrato en *Blockchain* combate el fraude.

Seguro en el automóvil

La combinación de Internet de las Cosas con *Blockchain*, las aseguradoras contando con esta tecnología, podrán procesar información segura y confiable de los datos del conductor que quiera asegurar su vehículo porque el historial de siniestros fueron registrados en *Blockchain*. Y luego procesada y analizada la solicitud de acuerdo a los criterios de evaluar el riesgo de la aseguradoras, el cliente podrá recibir varios contratos inteligentes con ofertas distintas.

2.3.4 Descentralización

Descentralización de Internet

Actualmente se hace uso de Internet con un *DNS* (*Domain Name System*) para resolver páginas de Internet, donde la empresa *Dyn* es uno de los grandes proveedores de *DNS* y el 21 de Octubre de 2016 esta empresa sufrió un fallo de seguridad dejando sin acceso a varias páginas de Internet durante horas en algunas zonas de Estados Unidos.

También se hace uso hoy en día de certificados para hacer seguras las páginas en internet *HTTPS*. Los certificados son emitidos por pocas empresas y grandes como por ejemplo *Verisign*.

Y un último componente importante en internet es la identificación y autenticación de usuarios. Donde muchas personas se identifican en internet con servicios como las grandes empresas *Google* y *Facebook* y hacen uso de otros servicios con el mismo usuario y contraseña utilizadas en esas grandes empresas.

Con *Blockchain* se trata de evitar la centralización de *DNS*, certificados de seguridad para páginas y la autenticación de usuarios en servicios de Internet.

Existe una búsqueda de Internet descentralizado con la empresa *Blockstack* donde se cuenta con un proyecto de protocolo descentralizado de código abierto.

También existe el protocolo *IPFS* (*Inter Planetary File System*) desarrollado por *Protocol Labs* que trabaja en un almacenamiento descentralizado. Como así también existen otros protocolos *Permacoin, Factom* y *Storj* experimentando en la misma línea de *IPFS*.

En vez de un almacenamiento centralizado de archivos como las existentes actualmente, *Dropbox ,Amazon* o *Google Drive* ,la tecnología *Blockchain* puede ser usada para el almacenamiento distribuido y descentralizado de datos o archivos en una configuración de red *P2P* (red de pares) , constituido por múltiples miembros.

Es decir un almacenamiento distribuido tiene múltiples copias en distintos lugares de la red siendo así el sistema más seguro. En los sistemas centralizados toda la información es de facilidad de ataque por un hacker o se pierda la información por algún problema técnico, catástrofe natural o algún accidente no natural.

Los *DNS* (*Domain Name System*) en la actualidad se encuentran bajo control centralizado y son vulnerables a abuso de poder, de censura o de espionaje de lo que el usuario haga de internet. Con el uso de la tecnología de *Blockchain*, los *DNS* permanecerían de forma descentralizada tal que cada usuario tenga el mismo listado de *DNS* en la computadora.

Existe el proyecto *NameCoin* con tecnología de *Blockchain* con código abierto y es experimental para implementar una versión descentralizada de los *DNS*.

Se piensa también en el uso de *Blockchain* para cambiar la gestión y distribución centralizada de certificados digitales que son emitidos por una autoridad central (infraestructura de claves públicas llamada PKI) y en su reemplazo llevar a un tipo de infraestructura descentralizada llamada KSI (*Keyless Security Infraestructure*).

Procesos electorales

Se pueden resolver los problemas de los sistemas de votación con la tecnología de *Blockchain* respecto al anonimato del voto y así una persona no pueda votar más de una vez, garantizando la privacidad del voto. También no es posible la manipulación porque no hay una autoridad central para gestionar el sistema de votación. El uso del voto electrónico con *Blockchain* mejora la rapidez y reduce los costos de elecciones y referéndums en los gobiernos de países. Pero la utilización de votación mediante *Blockchain* también podría ser utilizado dentro de una consulta interna en una compañía.

El partido político danés llamado *Liberal Alliance* realizó la primera votación con *Blockchain* en el año 2014, esta fue una elección interna.

En Australia se estudió también el uso de *Blockchain* en los procesos electorales.

Descentralización del Internet de las Cosas

Para la interconexión de dispositivos se puede usar *Blockchain* para el intercambio de datos en forma segura y registrando todos los mensajes intercambiados, evitando el control centralizado de las conexiones que la mayoría de las plataformas *IoT* lo hacen.

IBM junto a *Samsung* crearon una plataforma llamada *ADEPT* (*Autonomous Decentralized To Peer Telemetry*), esta es una red de dispositivos distribuida usando *Blockchain* con tres protocolos:

- *Bittorrent* para compartir archivos.
- *Ethereum* para los *Smart Contracs*.
- *Telehash* para la mensajería *P2P*(red entre pares).

La *startup Filament* creó un software para IoT(Internet de las Cosas) descentralizado usando *Blockchain* de *Bitcoin* donde cada dispositivo tiene un identificador único.

2.3.5 Gestión de identidades

Con *Blockchain* los usuarios pueden crear su identidad digital a prueba de manipulación, que reemplaza a los nombres de usuario y contraseña. Haciendo uso de este tipo de identidad digital para el acceso a aplicaciones, sitios *web* y firma de documentos digitales.

Existen compañías que ofrecen estos servicios como *Onename, ShoCard* y *Keybase*.

Una iniciativa llamada *Blocchain Emergency ID* de *Bitnation* , consiste en proporcionar una identificación digital de emergencia para los inmigrantes y refugiados que tengan pasaportes confiscados o extraviados.

En este tipo de aplicación se crea una red de confianza en el que los miembros de cada familia pueden verificar las identidades de los miembros.

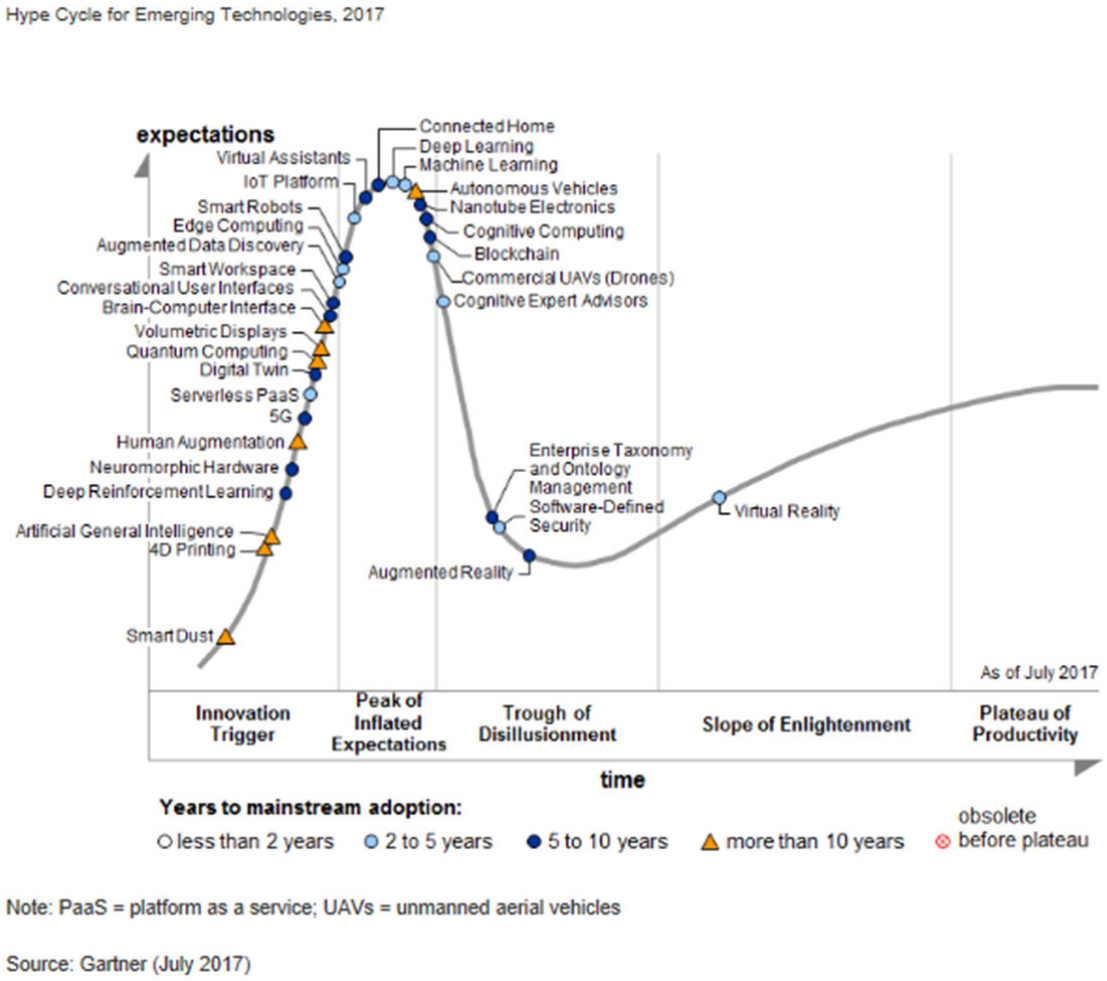
2.4 Curva de *Gartner*

El *Hype Cycle* de *Gartner* es una representación gráfica de la madurez y adopción de tecnologías y aplicaciones. Proporciona una perspectiva de las tendencias de las industrias tecnológicas emergentes y ayuda a discernir si estamos en presencia de una sobreexpectación o ante una tecnología viable.

El *Hype Cycle* nos brinda una visión de cómo una tecnología evolucionará en el tiempo y así se tendrá una visión de la penetración de la nueva tecnología. Está compuesto por cinco fases relevantes del ciclo de vida de una tecnología y son el lanzamiento (disparador de la innovación), el pico de las expectativas infladas, el abismo de la desilusión, la rampa de la consolidación y por último la meseta de la productividad.

El *Hype Cicle* de *Gartner* de Julio de 2017 muestra en la Figura 2.6 a la tecnología *Blockchain* en desarrollo en la fase tres, dejando el pico inflado de expectativa y está en evolución a adoptar de 5 a 10 años.

Figura 2.6: Gráfico de *Gartner* de tecnologías emergentes



Fuente: Smart Gartner (2017)

2.5 Casos de uso no financieros por sectores

En el siguiente Cuadro 2.2 se resume los distintos casos de uso con iniciativas en los sectores Público, Privado y las ONG, donde se observan empresas y gobiernos de países llevando a cabo el desarrollo de *Blockchain* con las distintas aplicaciones y plataformas.

Cuadro 2.2: Casos de uso en sectores

		Sector Privado	Sector Público	ONG
Casos de uso	Registros	Tieron,Mediachain.io ,CoalaIP.org,Factom, Monegraph,Verisat,Blockchai,Slack,Stampery, Blockverify, Ascribe, Uproov y Proof Existence de Bitcoin	Estonia,Dubái,Honduras, Australia, Giorgia,Ghana, Japón,India, Rusia,Suecia, Singapur,Brasil,Ghana y USA	
	Trazabilidad	Provenance.Org, SkuChain y Everledger	Finlandia	Homeless,Entrepreneur,It-willbe.org,Fundación Recover,KUBUKA,Farmacéuticos sin Fronteras, Fundación Exit, Orden de Malta y Cáritas
	Contratos	Power Ledger, LO3, ConsenSys,RWE, Slock.it,La'Zooz,Grid Singularity,Aegon, Allianz, Munich Re, Swiss Re y Zurich.		
	Sistema de Votación		Rusia,Dinamarca,Corea del Sur, Sudafrica, Ucrania , USA y Australia	
	Gestión de Identidad	Onename, ShoCard , Keybase y Bitnation		
	Descentralización de Internet	Blockstack,Storj, Tahoe-LAFS , Datacoin,Protocol Labs, Namecoin y Factom		
	Internet de las cosas	IBM,Samsung y Filament		
	Aplicaciones Militares		USA y OTAN	

Fuente: Elaboración propia

De todos los casos de uso, uno que resalta en el cuadro anterior es el Registro y Verificación en el sector público. Países como Australia, Brasil, Estonia, Dubái, Honduras, Giorgia, Ghana,Japón, India ,Rusia, Singapur, Suecia y USA han empezado a experimentar el uso de *Blockchain* en registros públicos.

Y en el desarrollo de este trabajo es de interés mencionar el caso de uso *Proof of existence* (Prueba de Existencia) porque permite comprobar la existencia de cualquier documento registrado en la *Blockchain,* aportando valor agregado a los procesos de registros en el organismo público, por lo que es de importancia su estudio.

2.6 *Proof of existence*

Proof of existence es un caso de uso de verificación de registro de archivos y guarda solo el *hash* en la red *Blockchain* de *Bitcoin*.

Figura 2.7: Logo de aplicación Prueba de Existencia en *Bitcoin*

Proof of Existence

Written forever.

Fuente: Sitio docs.proofofexistence.com

La prueba de Existencia se usa para registrar cualquier archivo de computadora sobre una red de *Blockhain* de *Bitcoin*, generando un digesto que sirve como comprobante de registro.

Esta aplicación actualmente se encuentra operativa en el sitio *web* del cual uno puede registrar cualquier archivo y tiene un costo de 0,00025 BTC equivalente a 211,552 pesos argentinos.

Este servicio *online* llamado *Proof of Existence* sirve para patentes, registro de autor, integridad del archivo y lo que se llama *Time Stamp* (este contiene una fecha y hora de lo registrado).

Proof of Existence de BFA

En Argentina existe la plataforma Blockchain Federal Argentina donde se pueden volcar aplicaciones, tal como la Prueba de Existencia y también la posibilidad realizar casos de uso diferentes. Desde el 2018 se fueron sumando distintos sectores con distintas iniciativas de casos de uso.

El caso de uso inicial de la BFA fue el Sello de Tiempo , este permite certificar contenidos permitiendo la generación de prueba de existencia , es decir un sello digital que demuestra el contenido registrado en la *Blockchain* y fue hecho en una fecha , hora determinada y no tuvo modificación.

Blockchain Federal Argentina brinda la posibilidad de utilizar el sellado de tiempo de acuerdo a las necesidades y posibilidades de cada usuario.Dispone en el sitio de la *gitlab.bfa.ar* de forma pública de una aplicación denominada *TSA API* que interactúa con un *Smart Contract* para certificar todo tipo de archivos o documentos.

El caso de *Proof of Existence* se realizó en BFA el cual uno puede encontrar el desarrollo y mejora de los códigos abiertos en el sitio de *Gitlab*.

Los desarrollos en BFA son:

- *Smart Contract* que contiene el caso de uso *Proof of Existence*
- *TSA API* que invoca al *Smart Contract* de *Proof of Existence*

Smart Contract

El contrato inteligente que contiene la Prueba de Existencia, consta de funciones de relevancia para impactar, verificar y obtener datos de registro en la *Blockchain*. El *Smart Contract* se programa en el lenguaje *Solidity*:

- *function stamp( ):* La función *stamp* realiza el impacto del *hash* en la red *Blockchain* para registrar en un bloque.

- *function verify( )* : La función *verify* realiza la verificación de que exista el registro en un bloque a un *hash* correspondiente.

- *function getHash( )*: La función *getHash* devuelve el *hash* correspondiente del registro consultado.

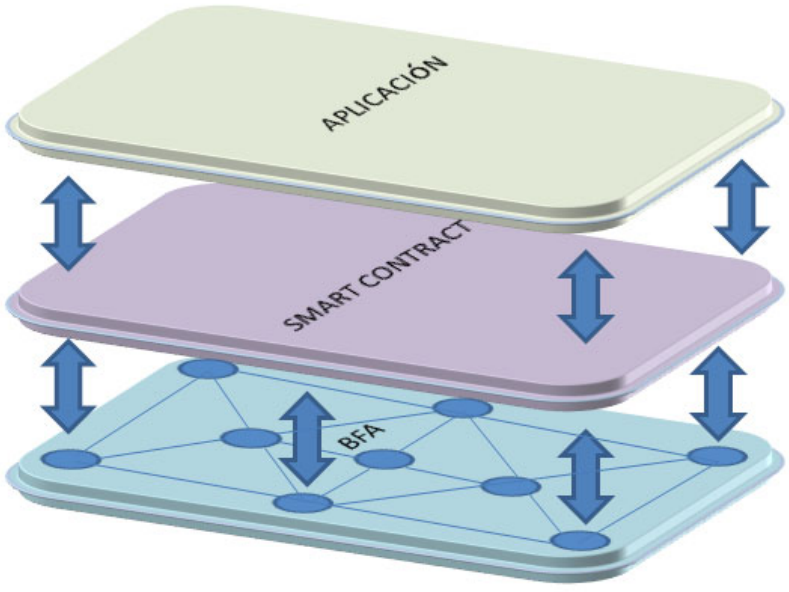
- La función *getBlockNumber* devuelve el número de bloque del registro consultado.

TSA API

En un programa en *Python* ejecutado en *Ubuntu* queda instalada la aplicación denominada *TSA API* que interactúa con el *Smart Contract* desplegado en la red *Blockchain.*

La función de la aplicación es que el usuario interactúe con el *Smart Contract* y la red de *Blockchain*, luego se lleve a cabo el proceso de registro en bloques y en la siguiente Figura 2.8 se puede ver como el *Smart Contract* está desplegado y arriba de este, está la aplicación llamada *TSA API*.

Figura 2.8 : Capas de *Blockchain, Smart Contract* y Aplicación



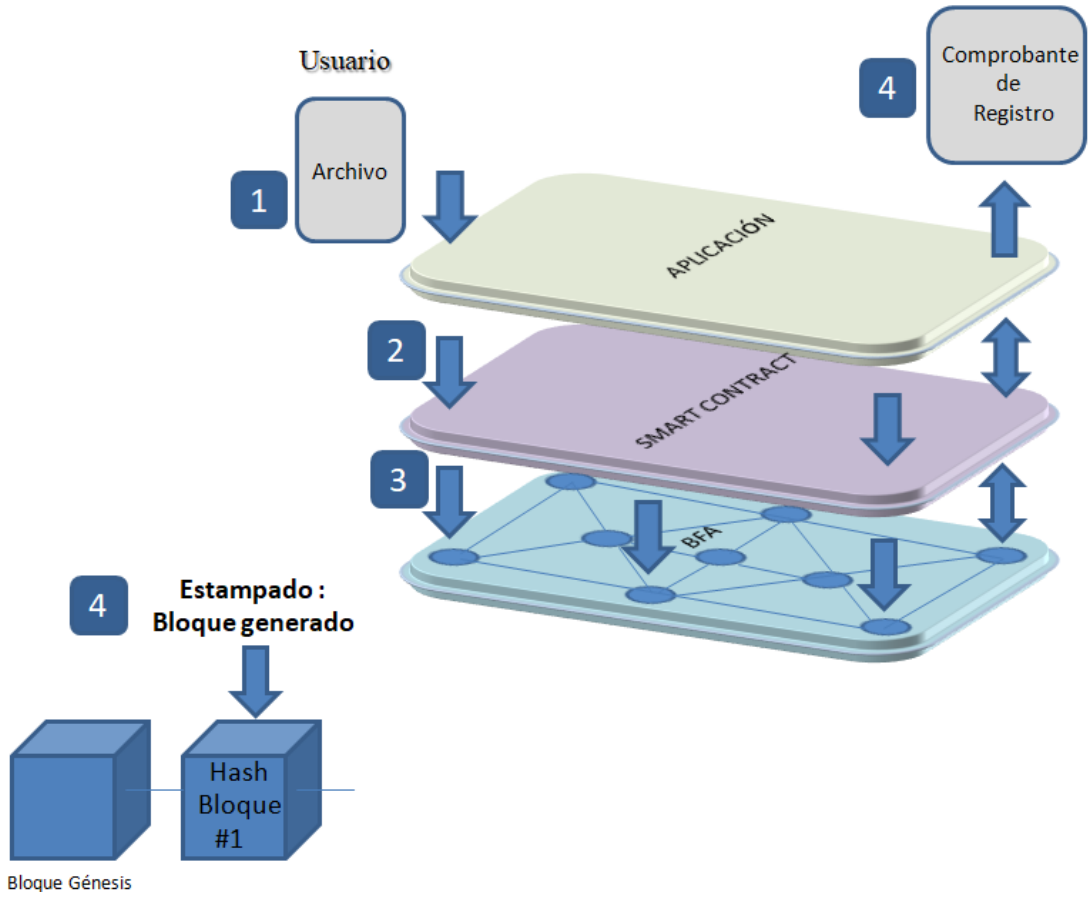
Fuente: Elaboración propia

Procedimiento de estampado Figura 2.9:

1. Usuario mediante la aplicación inserta el documento o archivo a registrar.
2. La aplicación llama a la función *stamp* del *Smart Contract*.
3. El *Smart Contract* entrega el *Hash* a la red de *Blockchain.*
4. Se inserta el *hash* en el bloque de la cadena y se entrega al usuario el comprobante de registro.

El comprobante contiene el *Hash*, el algoritmo usado para realizar el *hash*, el número de bloque, la fecha y hora que se registró en el bloque y la dirección del contrato desplegado en la red Blockchain.

Figura 2.9: Proceso de insertado de *Hash* en un Bloque

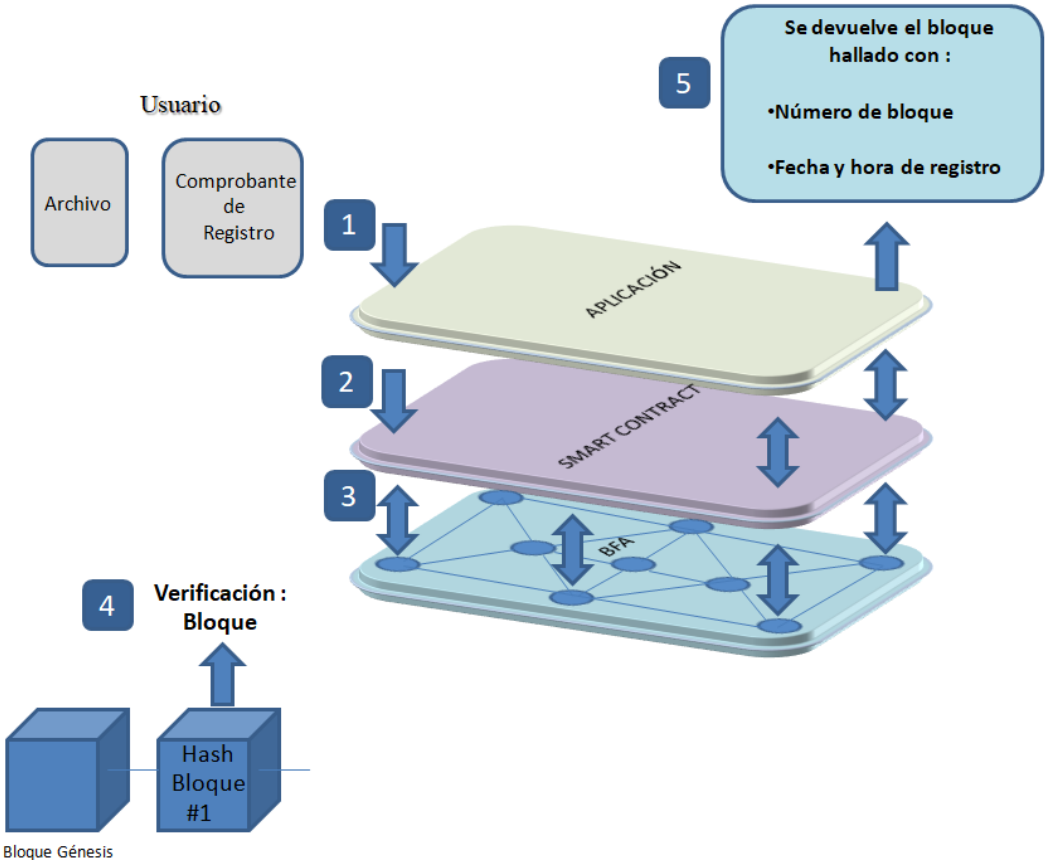


Fuente: Elaboración propia

Procedimiento de verificación Figura 2.10:

1. Se inserta el comprobante y el archivo a verificar en la aplicación *Blockchain* BFA, se calcula el *Hash* del archivo para luego comparar con el Hash del comprobante. De darse la coincidencia de ambos Hash se sigue con el paso 2. De lo contrario la aplicación informa que el comprobante no corresponde con el archivo.
2. La aplicación dialoga con el *Smart Contract* a través de la función *verify*.
3. El *Smart Contract* verifica en la red si existe tal bloque con el hash correspondiente al archivo.
4. De darse correctamente con el bloque buscado, se entrega al usuario a través de la función *getBlockNumber* el número de bloque correspondiente al *hash* del archivo.

Figura 2.10: Proceso de verificación de *Hash* insertado en un bloque



Fuente: Elaboración propia

Capítulo 3. Implementación de Blockchain en Prefectura

3.1 Internet en Prefectura Naval Argentina

La Prefectura Naval Argentina forma parte de LACNIC, cuenta con un número de sistema autónomo y direcciones públicas, conectándose así a la red de Internet mediante el protocolo BGP (*Border Gateway Protocol*). Luego en la Institución del Edificio Guardacostas se vino trabajando en la optimización del servicio de Internet, todo esto en el área de División de Redes de la Prefectura Naval Argentina. A continuación se describirá cómo fue posible optimizar la red.

Prefectura Naval Argentina miembro de CABASE IXP Buenos Aires

La red del Edificio Guardacostas es miembro conectado al IXP Buenos Aires, los *IXPS* son puntos de la red de Internet (*Internet Exchanges Points* o también llamados *NAPS Network Access Points*) y son fundamentales porque pertenecer a estos puntos hace más rápido el intercambio de tráfico entre redes de diversas entidades (operadores, proveedores de acceso, organismos de gobierno, entidades académicas, etc).

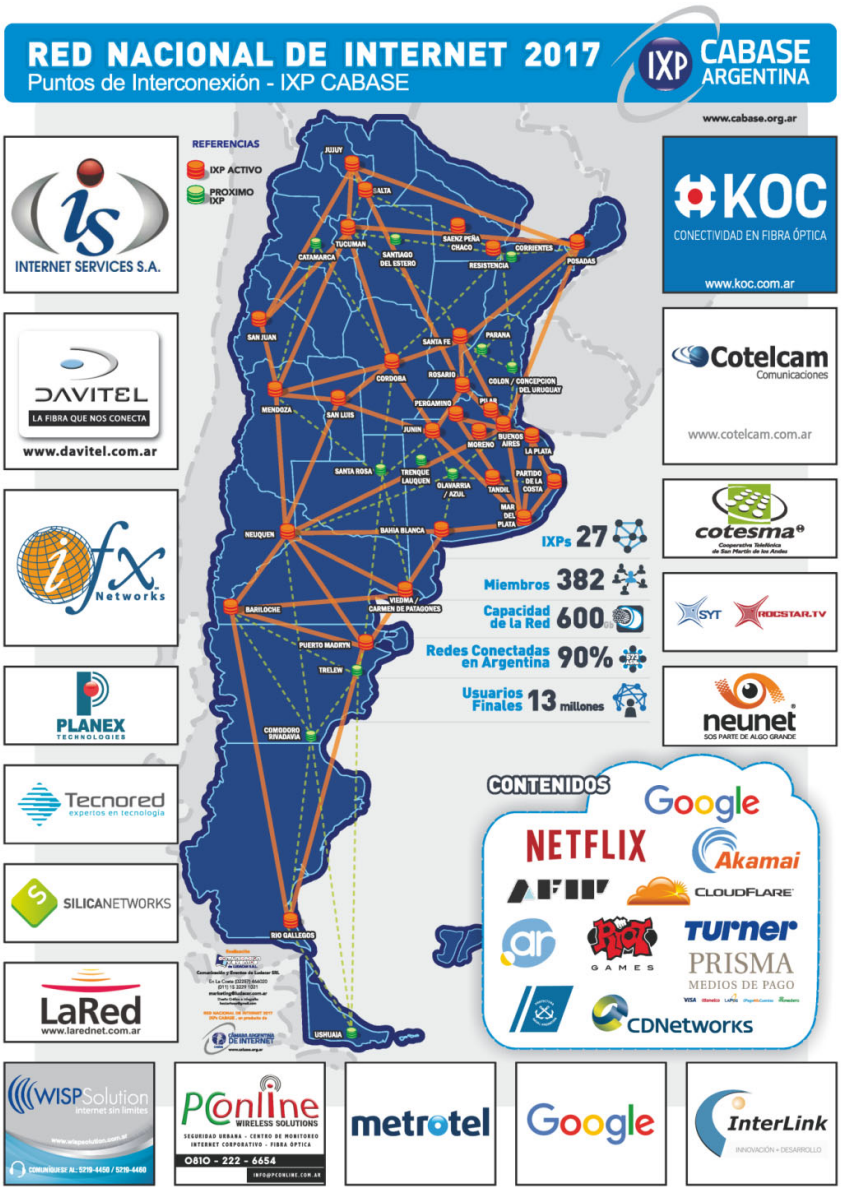
En el mundo también están presentes *IXPS* bajo distintos esquemas institucionales, topológicos y operacionales.

Por eso la importancia de que la Prefectura Naval Argentina es ya parte del punto de intercambio *IXP* Buenos Aires CABASE, logrando eficiencia en el ruteo de internet, mejorando la calidad servicio y minimizando los costos de interconexión. En sí se mejora la calidad en las comunicaciones.

CABASE es la Cámara Argentina de Internet que trabaja desde 1989 promoviendo el desarrollo de las telecomunicaciones en Argentina y está reconocida mundialmente como entidad argentina referente de Internet. Además de ser un asociado a CABASE, y los puntos de intercambio, la Prefectura Naval Argentina en el Edificio Guardacostas se suma también a los *cachés* de *Google* y *Akamai* en el NAP Buenos Aires.

La importancia de tener los *cachés* de *Google* y *Akamai* es porque a nivel mundial el 80% de la red está relacionado con contenidos de *Google* y *Akamai* y entre otro tráfico, que hacen al mayor consumo de Internet y contar con servidores *cachés* de consumo cercano sin ir a buscar a otros *carriers* (empresas que ofrecen rutas de conexión a internet) en otros continentes, se logra la optimización del tráfico en velocidad.

Figura 3.1 : Mapa de puntos *IXPS* CABASE Argentina



Fuente: Sitio cabase.org.ar

Un ecosistema de nodos miembros conectados en la mejora de Internet hasta el presente como es CABASE permitió desarrollar proyectos con distintas entidades de Argentina.

Entre ellos, surge implementar una innovación tecnológica de parte de NICar , ARIU y CABASE que dieron el inicio de la plataforma de Blockchain Federal Argentina.

Dada la importancia de las aplicaciones de *Blockchain* mas allá de las criptomonedas y enfocando al uso de caso de registro y verificación de datos, la Prefectura Naval Argentina se incorpora como primera autoridad marítima para ser parte de la plataforma multiservicios de la Blockchain Federal Argentina y con la intención de su uso en la institución en el proceso de registros como es la iniciativa de aplicación de este capítulo del Certificado de Altura de Ríos.

3.2 Prefectura Naval Argentina como parte de BFA

Unir un nodo de Prefectura a la red o plataforma multiservicios de BFA, trae cuestiones administrativas y técnicas a considerar.

Parte administrativa consta de:

- Solicitud de incorporación como parte
- Reglamento Interno de la BFA
- Consejo de Administración
- Políticas de uso de la BFA
- Operación de la red

Parte técnica consta de:

- Procedimiento de incorporación de nodo sellador de Prefectura Naval Argentina.
- Procedimiento de incorporación de un nodo transaccional.
- Herramientas para el despliegue de *Smart Contracts*.

3.2.1 Parte administrativa

Reglamento Interno de la BFA

Se establece un reglamento para las normas de funcionamiento de la BFA siendo esta una plataforma multiservicios de alcance federal con implementación de una infraestructura *Blockchain.*

Siendo esta plataforma BFA de características:

- Semipública y permisionada
- No tendrá criptomoneda asociada
- Basado en un consenso liviano sin competencia de generación de bloque
- Infraestructura a cargo de las partes de forma colaborativa
- Las transacciones serán gratuitas
- Código abierto

Siendo así la Prefectura Naval Argentina procedió a formar parte a la plataforma, constituida por los sectores:

- Academia
- Industria y Comercio
- Gobierno Nacional
- Gobiernos Provinciales y de la Ciudad Autónoma de Buenos Aires
- Sociedad Civil

Solicitud de incorporación

Mediante un formulario de Solicitud de Incorporación en este caso la Prefectura Naval Argentina acuerda ser parte de la red Blockchain Federal Argentina.

Consejo de Administración

Ser parte de la red, lo decidirá el Consejo de Administración de BFA que instrumenta el mecanismo de aprobación de incorporación de nodos de la red.

Operación de la red

La función de las partes de BFA en la infraestructura de la red es contar con nodos que agreguen bloques de transacciones de la *Blockchain*, así cada nodo (miembro parte de BFA) se denomina con el nombre de nodo sellador.

Los nodos selladores son la parte del *core*, es decir la estructura central de la red confiable de BFA y son los únicos que hacen participación en el proceso de consenso para agregar bloques a la cadena con cuentas validadas por cada nodo sellador.

Los selladores rechazarán o descartarán conexiones de otros nodos en la red y no se contactarán con nodos que no sean selladores o que no sean nodos intermediarios como *gateways* o *bootnodes-core*, creando así una red eficiente y confiable.

Los nodos selladores tienen comunicación entre sí en forma de red *mesh*:

- Sin necesidad de todos contra todos
- Pueden contactarse con los demás nodos selladores y nodos intermediarios.

Políticas de Uso de la BFA

De acuerdo a las políticas de uso de BFA al cual PNA es parte, también se hará uso de un nodo transaccional para la aplicación a desarrollar como Certificado de Altura de Ríos.

El *ether* es asignado en forma periódica por el Consejo de Administración para poder realizar transacciones y estas son agregadas como bloques por los nodos selladores.

Pasado el acuerdo de unirse como institución con los otros organismos privados y públicos, se pasa al análisis técnico y a los procedimientos de cómo instalar un nodo de la institución dentro la Prefectura y así se pueda contar con una plataforma para volcar casos de uso basados en *Blockchain.*

3.2.2 Parte técnica

Procedimiento de incorporación de nodo sellador de Prefectura Naval Argentina:

En Prefectura se contará con un servidor donde se instalará una máquina virtual con capacidades acorde a los requisitos técnicos que indica BFA, mostrado en el Cuadro 3.1

Cuadro 3.1: Especificaciones técnicas para el Nodo sellador y Nodo transaccional

CPU	Datos Técnicos
Procesador	2Vcpu
Memoria	4GB de RAM
Disco Rígido	300Gb a 1TB
Máquina Virtual	Debian/Ubuntu
Dirección IP	IPv4 fija y pública
Puertos	30303/TCP y 30303/UDP

Fuente: Adaptado de Documentos sobre BFA Requerimientos Técnicos para Nodos

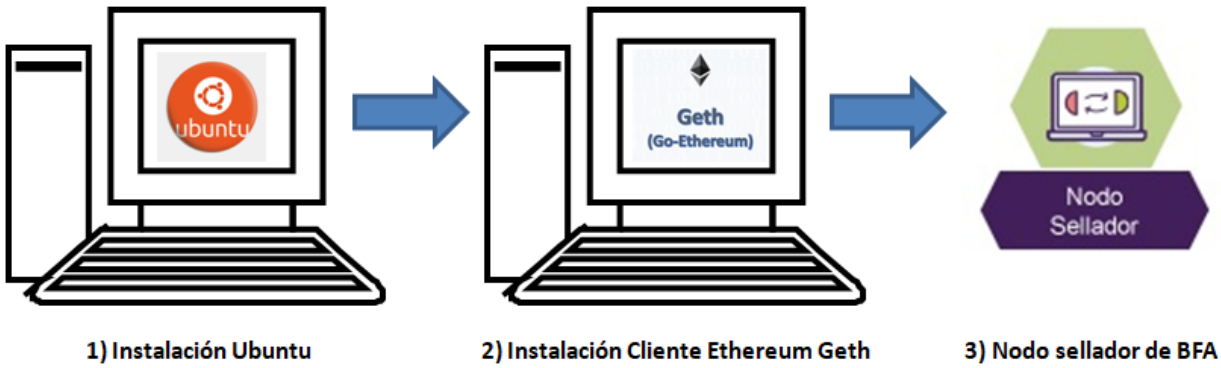
Entonces el procedimiento del Nodo Sellador será :

1) Se instala Ubuntu.

2) Incorporación del nodo con la instalación del cliente *Ethereum* llamado *Get* en la máquina virtual con el *Ubuntu* instalado anteriormente.

3) Una vez instalado el cliente *Get*, se genera en este un número de cuenta, este se registra en la página de BFA (www.bfa.ar) y luego del registro se obtiene el *ether* para realizar transacciones.

Figura 3.2: Instalación de Nodo Sellador en BFA



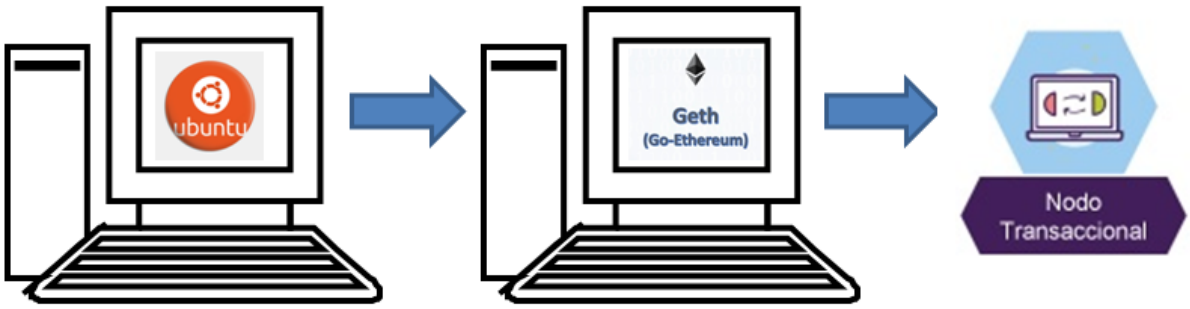
Fuente: Elaboración propia

Procedimiento de incorporación de un nodo transaccional:

También se requiere de otra instalación de una máquina virtual con los requisitos que muestra el Cuadro 3.1

Para el nodo transaccional también se genera una cuenta, instalando un cliente *Ethereum* en otra máquina virtual *Ubuntu*. Se sigue misma secuencia del caso anterior de Instalación de Nodo Sellador pero con la diferencia del paso 3) donde se generará una cuenta de Nodo Transaccional y este tendrá el *ether* otorgado por la BFA con el registro en el sitio web de BFA.

Figura 3.3 : Instalación de Nodo Transaccional en BFA



Fuente: Elaboración propia

3.3 Implementación de la aplicación en BFA

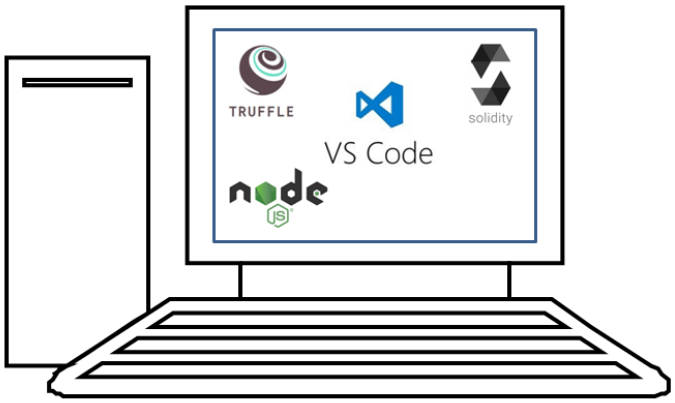
La aplicación se instalará sobre el nodo transaccional y para su realización se necesitará previamente de herramientas o un entorno de desarrollo para desplegar el *Smart Contract*.

3.3.1 Herramientas

Se hará uso de *Visual Studio Code* y *Node js* (Versión 8) para desplegar el *Smart Contract* en la red BFA y será de importancia para el funcionamiento de la aplicación a concretar como iniciativa en PNA.

Se va usar una PC de entorno de desarrollo de aplicaciones y se instalan el *Visual Studio Code , Node Js, Truffle* y *Solc*.

Figura 3.4: Instalación del entorno de desarrollo



Fuente: Elaboración propia

El *Visual Studio Code* es un editor de código fuente desarrollado por *Microsoft* para *Windows, Linux y macOS*. Este será el entorno de trabajo para compilar, probar y desplegar contratos inteligentes en la red *Blockchain*.

Junto al *Visual Studio Code* se instala el *Node.js* para la ejecución de programas escritos en *JavaScript*.

Luego se agregan al entorno otros complementos necesarios para despliegue de *Smart Contracts:*

- *Truffle* : Herramienta de desarrollo
- *Solc:* Compilador de Solidity

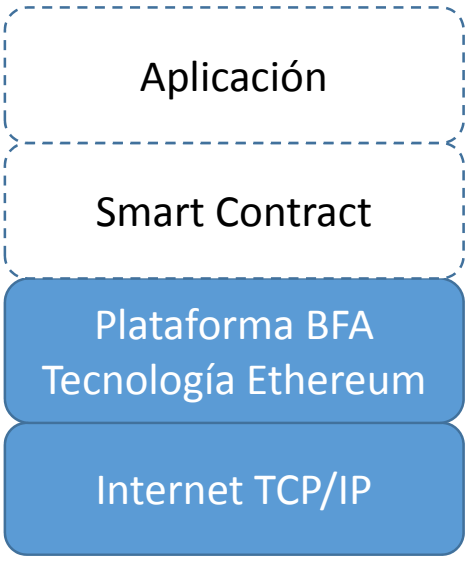
Se instala *Truffle* que es un conjunto de herramientas que permite crear aplicaciones sostenibles y profesionales en cualquier *Blockchain* usando la Máquina Virtual de *Ethereum.*

Y por último se instala *Solc* que es el compilador de lo que se programe en el lenguaje de código de *Solidity* que es usado para los *Smart Contracts*.

Finalmente se integra de esta forma todas las herramientas necesarias para trabajar en el entorno de *Visual Studio Code.*

Una vez que se tienen las herramientas y los nodos instalados, se procederá a insertar el Contrato Inteligente siguiendo el siguiente modelo de capas:

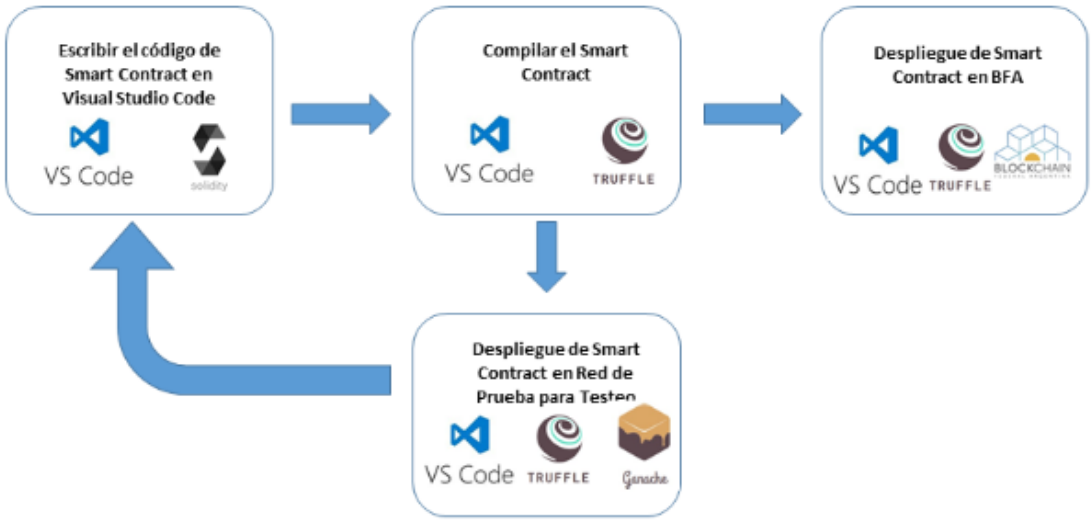
Figura 3.5: Capas para la aplicación blockchain



Fuente: Elaboración propia

Según la Figura 3.5, después de tener el *Smart Contract* desplegado, se aplicará lo que comprende la aplicación que va interactuar con el contrato inteligente. El *Smart Contract* a insertar contiene el *Proof of Existence* de BFA pero antes se realizan inserciones con contratos inteligentes de prueba para comprobar el correcto funcionamiento de las herramientas, entornos de trabajo y el nodo sellador. Es decir si realmente se puede desplegar contratos con el entorno de trabajo de *Visual Studio Code*. El *workflow* a seguir es:

Figura 3.6: *Workflow* de inserción de *Smart Contract*



Fuente: Elaboración propia

Luego de desplegar con éxito el *Smart Contract* de Prueba de Existencia, se instala la aplicación de *TSA API* de BFA en el nodo transaccional, que servirá para interactuar entre el usuario y el contrato inteligente.

3.3.2 Registro y publicación de Altura de Ríos en la web

La Prefectura Naval Argentina cuenta con su página oficial en el cual brinda información como autoridad marítima, entre ellas de importancia y en contexto al actual desarrollo de este trabajo, la publicación diaria del estado de los Ríos con información actualizada. Con fuentes de los datos de lectura de hidrómetros argentinos, leídos por la Prefectura Naval Argentina y los valores están expresados en Mts. También hay datos suministrados por Brasil mediante las diferentes administraciones y autoridades brasileñas a cargo de las represas respectivas.

En la siguiente imagen es una captura del sitio web del mapa de altura de ríos donde los círculos con diferentes colores corresponden a los distintos lugares donde se toman las medidas de altura de ríos:

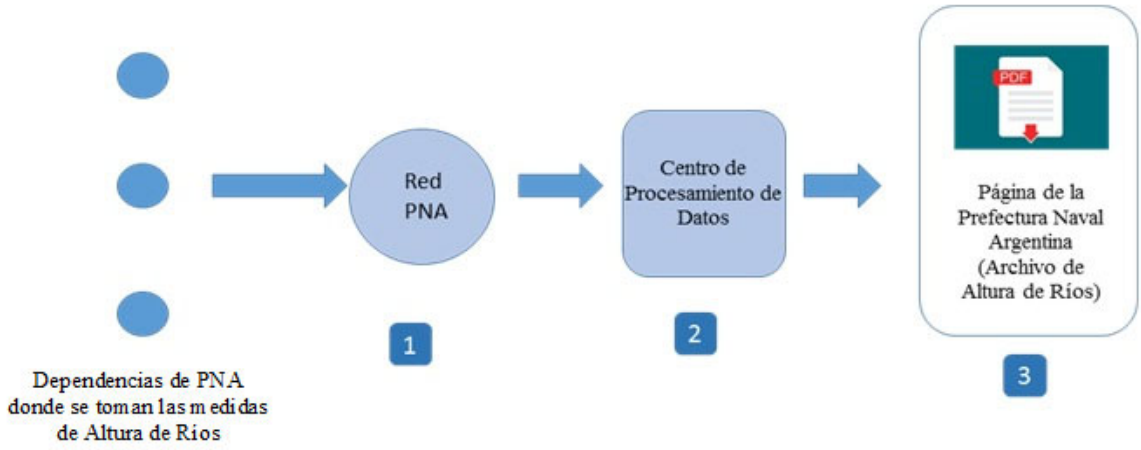
Figura 3.7: Mapa de estado de los Ríos

Fuente: Sitio contenidosweb.prefecturanaval.gob.ar/alturas

En el sitio web de prefectura se puede descargar el documento *pdf* con la información del estado de los ríos de todos los sitios del mapa con fecha y hora. El proceso de registro se explica a continuación.

Proceso de registro de documentos Altura de Ríos:

Figura 3.8: Proceso de generación de documentos



Fuente: Elaboración propia

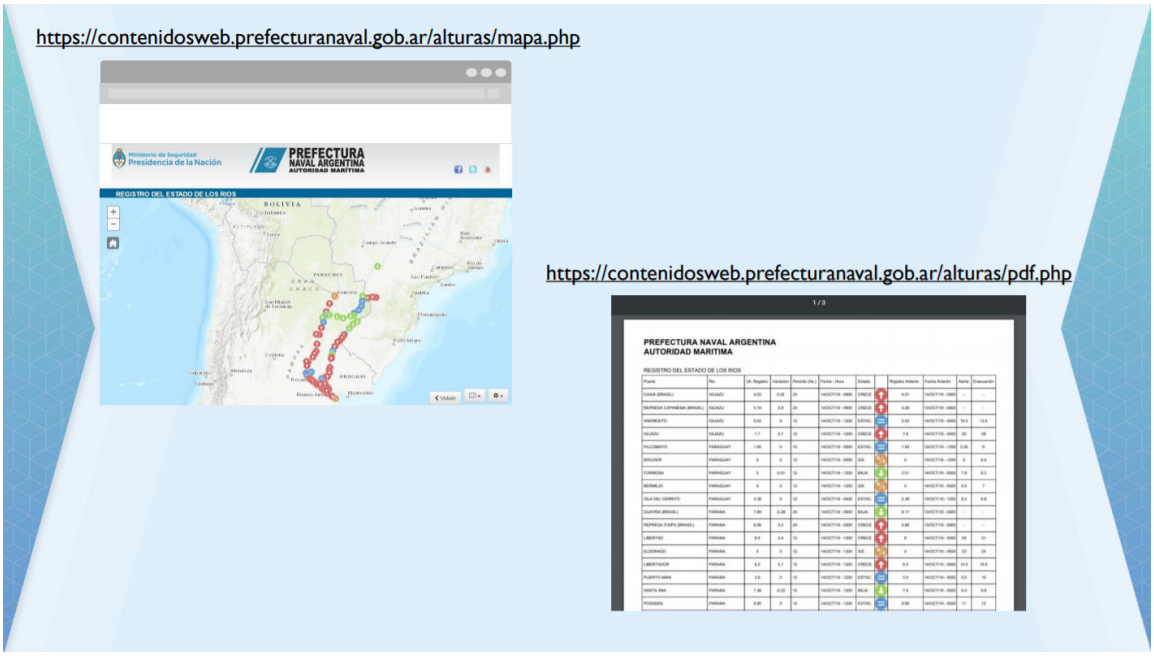
1) Desde distintas dependencias de PNA se toman las medidas de altura de Ríos en forma diaria. Y se envían mediante Internet, llegando a la red de PNA (Prefectura Naval Argentina) del Edificio Guardacostas.

2) En el Edificio Guardacostas en el sector de procesamiento de datos se juntan todos los documentos de altura de Ríos, se tiene un histórico de las medidas y se digitaliza en un archivo pdf.

3) Se publica en la página oficial de la Prefectura Naval Argentina el pdf con todas las medidas de los hidrómetros.

Y en la imagen siguiente se puede ver el mapa y el archivo pdf que brinda la información del estado de los ríos.

Figura 3.9: Mapa y documento pdf de los registros de Altura de Ríos



Fuente: Sitio contenidosweb.prefecturanaval.gob.ar/alturas

Conocer la Altura de Ríos es de suma importancia para el navegante, el ribereño, el Instituto Nacional del Agua (INA) y para las cargas y descargas de mercadería de buques y barcazas en la Hidrovía Paraná-Paraguay.

3.3.3 Impacto de los registros de altura de ríos

Es importante conocer la altura de los ríos para saber cómo pueden afectar a los ribereños y a las embarcaciones.

Y de las embarcaciones más relevantes es la que se relaciona con la Hidrovía Paraguay-Paraná (Figura 3.10) porque involucra el comercio, las exportaciones e importaciones.

Figura 3.10: Hidrovía Paraguay-Paraná

Fuente: Bolsa de comercio de Rosario Informativo Semanal 5 de Enero 2018

La Hidrovía Paraguay-Paraná es una de las vías navegables naturales de mayor longitud del planeta con una extensión de 3422 km desde el puerto Cáceres (Brasil) a Nueva Palmira (Uruguay).En esta vía se encuentran los ríos Paraguay, Paraná y Uruguay .Y junto a las infraestructuras portuarias de Bolivia, Paraguay y Uruguay se conforma uno de los sistemas logístico-comerciales fluviales más importantes del mundo.

Hay una población de 40 millones de habitantes y también una gran superficie para el desarrollo integral y sostenible de la región con una producción basada en agroalimentos, minerales y productos industriales. Por lo tanto es muy significativo esta vía de transporte para el logro de la integración física y económica del Mercosur.

Las terminales portuarias de la Hidrovía Paraguay-Paraná como puede observarse en el Cuadro 3.2 son alrededor de 105 ubicadas desde Puerto Cáceres (Brasil) y hasta Gran Rosario con la inclusión de la zona del Alto Paraná, esta va desde Itapú y hasta Confluencia .De las cuales 29 están ubicadas en el Gran Rosario, siendo esta una infraestructura portuaria muy relevante para Argentina.

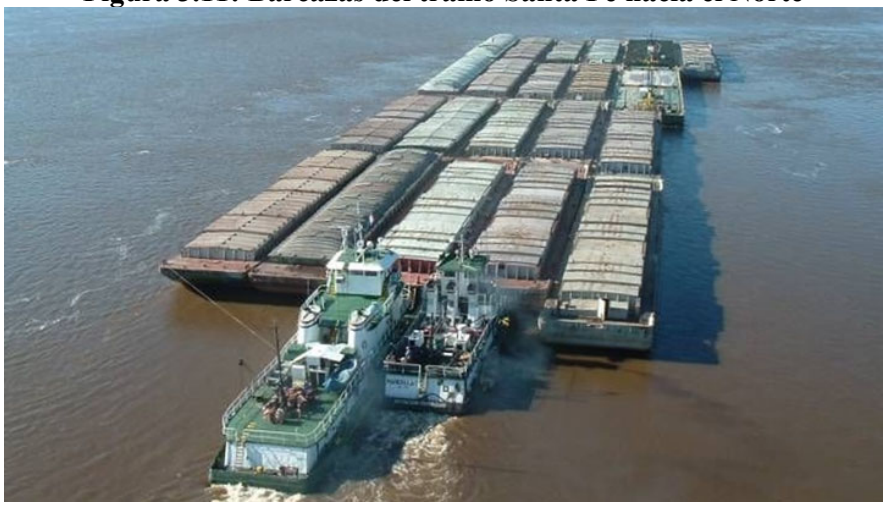
Cuadro 3.2: Puertos Hidrovía Paraguay-Paraná

Zona	Número de terminales portuarias
Terminales Portuarias en las secciones 1 y 2 de la Hidrovía Paraná- Paraguay (Tramo Puerto Cáceres-Confluencia).	51
En territorio de Bolivia	4
En territorio de Brasil	7
En territorio de Paraguay	39
En territorio argentino	1
Terminales Portuarias localizadas sobre el Alto Paraná (Tramo Itaipú- Puerto Iguazú- Confluencia)	16
En territorio de Paraguay	10
En territorio argentino	6
Terminales portuarias localizadas sobre el Río Paraná (tramo Confluencia- Diamante)	9
En territorio argentino	9
Terminales portuarias localizadas en el Gran Rosario	29
Total General	**105**

Fuente: Bolsa de comercio de Rosario Informativo Semanal 5 de Enero 2018

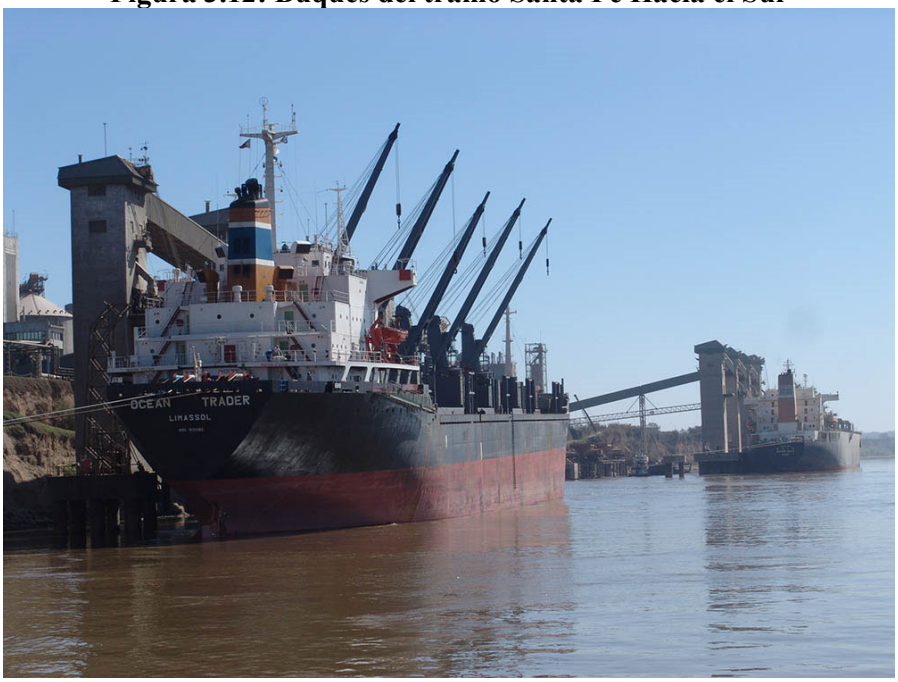
Desde el puerto de Santa Fe hacia el Norte solo pueden circular trenes de barcazas porque la profundidad del canal navegable está entre 7,10 y 12 pies. Luego desde la ciudad de Santa Fe hacia el sur operan factiblemente buques de ultramar debido que en ese lugar las profundidades son de 25 pies a más.

Figura 3.11: Barcazas del tramo Santa Fe hacia el Norte



Fuente: Sitio misionesonline.net

Figura 3.12: Buques del tramo Santa Fe Hacia el Sur



Fuente: Sitio rosarioesmas.com

Los 105 puertos es una cantidad relevante de infraestructura y esto evidencia el gran crecimiento de la Hidrovía en los últimos años. Siendo un enorme potencial hacia el futuro ,es mucho lo que puede crecer en los próximos años, donde se viene moviendo anualmente alrededor de 21 millones de toneladas de cargas pero pueden haber más crecimientos en el mediano y largo plazo. Donde lo más significativo de los últimos años fue:

- El crecimiento impresionante de la industria aceitera en el Gran Rosario desde el año 1995 se vino convirtiendo paulatinamente en el complejo oleaginoso más importante del mundo, siendo el nodo portuario de exportación de soja de mayor relevancia a nivel internacional en el 2016.

- La modernización y desarrollo notable de la infraestructura portuaria de Paraguay contando hoy con 49 terminales sobre los ríos Paraguay y Paraná.

- El gran crecimiento de la estructura industrial oleaginosa de Paraguay siendo el quinto productor mundial de poroto mundial de soja y el cuarto exportador mundial de poroto de soja.

- El desarrollo interesante de la infraestructura de los puertos localizados en Bolivia, estos son Gravatel Bolivia SA, Central Aguirre Portuaria y Puerto Jennefer.

  En el futuro el manganeso y el mineral de hierro pueden ser el aporte debido a que en la zona de Corumbá se encuentran los dos yacimientos más grandes como el Mutún y el macizo Ucrum. Se agrega además el crecimiento futuro de los niveles de actividad económica en esa zona con la posibilidad de generar grandes movimientos de cargas generales, contenedores, combustibles y otros productos.

El sistema de navegación natural de la hidrovía permite el transporte fluvial. Y depende mucho saber la altura del río Paraná para el transporte de la mercadería de barcazas y buques, involucrando a productores y consumidores con la posibilidad de ser afectados por el nivel del rio.

3.3.4 La bajante del Río Paraná y su impacto en el Gran Rosario

Importa saber en particular el puerto de Rosario donde se encuentra el complejo oleaginoso que depende mucho del nivel del Rio Paraná para el volumen de mercadería para la carga en los buques y el costo para los operadores del sistema logístico.

Para las medidas de altura de ríos, la Prefectura Naval Argentina usa la escala hidrométrica en el puerto de Rosario, esta fue colocada en 1884 por solicitud de la Bolsa de Comercio de Rosario (asociación creada ese mismo año). La Prefectura Naval Argentina (PNA) divulga las medidas de alturas de ríos. Y el Instituto Nacional del Agua (INA) aplica estas lecturas para pronóstico, ejemplo Cuadro 3.3.

El INA es un organismo científico tecnológico y tiene como objetivo el estudio, desarrollo ,investigación y prestación de servicios especializados en el campo de aprovechamiento y preservación del agua.

El Instituto Nacional del Agua usa las medidas de altura de ríos de PNA para pronósticos de los cambios de nivel en los próximos días. También con estas lecturas se realizan estudios y análisis de la dependencia de lluvias en las cuencas de Iguazú, Paraná Brasil, Uruguay y Litoral Argentino. Entre otros estudios del INA están de cómo los cambios del suelo y la variabilidad climática afectan a los niveles del río.

Cuadro 3.3: Pronóstico y Tendencia de Nivel de Río en Rosario

Estaciones	Nivel Hoy (*) (m) 17-feb-2021	Altura Media FEBRERO (1996 / 2020) (m)	Límite Aguas Bajas L (m)	Nivel de Alerta A (m)	Nivel de Evacuación E (m)	Pronóstico Preliminar (m) para 23-feb-2021			Estado	Tendencias (m) para el 02-mar-2021			Estado
						Mínimo	Central	Máximo		Mínimo	Central	Máximo	
CORRIENTES	3,62	4,27	3,00	6,50	7,00	3,70	4,09	4,40		2,90	3,58	4,00	
BARRANQUERAS	3,65	4,29	3,20	6,00	6,50	3,65	4,11	4,35		2,90	3,58	3,95	
GOYA	4,21	4,21	2,60	5,20	5,70	3,65	4,10	4,45		3,30	3,96	4,30	
RECONQUISTA	3,94	3,92	2,30	5,10	5,30	3,45	3,77	4,10		2,60	3,65	3,95	
LA PAZ	4,50	4,47	3,20	5,80	6,15	4,00	4,30	4,80		3,70	4,36	4,70	
PARANÁ	3,30	3,47	2,30	4,70	5,00	2,95	3,15	3,45		2,75	3,05	3,40	
SANTA FE	3,40	3,79	2,60	5,30	5,70	3,10	3,26	3,60		3,00	3,22	3,60	
ROSARIO	2,81	3,49	2,40	5,00	5,30	2,55	2,89	3,20		2,50	2,83	3,15	

" A ":Valores que superan el nivel de alerta " E ":Valores que superan el nivel de evacuación "L": Valores en aguas bajas (*): Dato de las 00:00hs

Fuente: Información de INA 17 de Febrero de 2021

Las escalas hidrométricas pertenecen a la Dirección Nacional de Coordinación Portuaria y Vías Navegables (DNCPVN).

El Gran Rosario se destaca en el territorio argentino como polo industrial-exportador de granos y subproductos. Siendo así de suma importancia para la economía de la República Argentina. Se ha potenciado desde la década de los 90 este polo por factores naturales y las

inversiones humanas. La vera del Rio Paraná tradicionalmente es el epicentro de la ubicación de puerto graneleros teniendo en la cercanía a la región más productiva en el cultivo de oleaginosas y cereales. Y además se cuenta con la desembocadura en el Rio de la Plata y luego al Océano Atlántico con las ventajas naturales de la barranca del río para la facilitación de la carga a granel. En esto se tuvo inversiones en dragado, recursos humanos, logística e infraestructura productiva configurándose un combo que potencia al Gran Rosario como principal polo industrial-exportador de la cadena agrícola.

Es de suma importancia como polo exportador el Gran Rosario, en el año 2016 superó a todos los demás clúster del mundo incluyendo al Distrito Aduanero de *Nueva Orleans* (USA) y el de Santos(Brasil).

En detalle el Mapa del Gran Rosario Figura 3.13, están los puertos y las plantas dedicados al proceso de semillas oleaginosas y a la exportación de sus subproductos, localizadas a lo largo de los 70 km de tramo de costa sobre el Río Paraná desde la localidad de Timbúes (al norte) hasta Arroyo Seco (sur).

Siendo en este tramo localizadas 29 terminales portuarias operando distintos tipos de cargas. Y de estas terminales ,19 despachan aceites, granos y subproductos, además 12 tienen plantas de molienda de oleaginosas teniendo al lado sus terminales portuarias. El complejo oleaginoso de Rosario cuenta con dos centrales termoeléctricas como San Martin y Vuelta de Obligado ubicadas en Timbúes. Además están ubicadas 2 terminales operando fertilizantes (Profetil y TFA), otra terminal despachando concentrados de cobre y oro como Minera Alumbrera , otras cinco terminales portuarias operando petróleo y sus derivados (Esoo, YPF,Petrobras, Oil Combustibles y en Arroyo Seco está Shell) y por último una terminal de multipropósito como la Terminal Puerto Rosario operando contenedores , cargas generales y aceites.

Figura 3.13: Mapa Gran Rosario

Fuente: Sitio http://biblioteca.municipios.unq.edu.ar/

Ante una bajante extraordinaria del Río Paraná el impacto tiene un peso de importancia y en consecuencia en la economía argentina porque este complejo agro-industrial exportador del Gran Rosario concentra el 80 % de capacidad teórica diaria de procesamiento de girasol y soja de Argentina. En el año 2019 desde las terminales portuarias del complejo se despacharon el 67% de los granos, el 93 % de aceites vegetales y el 96 % de harinas.

En el año 2018, entre Julio y Agosto hubo una bajante extraordinaria del nivel de rio Paraná y la medición en el puerto de Rosario fue de 0,5 metros por debajo de una referencia. Un fenómeno afectado por la falta de lluvias al sur de Brasil.

La empresa Hidrovía S.A. tiene el compromiso contractual de encargarse de las operaciones logísticas siempre y cuando se cumpla un valor de referencia de 2,47m del nivel del río en el puerto de Rosario.

Dado entonces el fenómeno de la bajante del 2018, el valor de referencia fue de 1,85m, esto afectó en los buques a cargar menos en el Gran Rosario implicando costos mayores logísticos y de transporte pasando a ser afrontados por los puertos, industrias y operadores.

Cuadro 3.4: Registro de Altura de Ríos entre Julio y Agosto del 2018

Fecha	Registro (Mts)
29/07/2018 12:00	1,85
29/07/2018 18:00	1,83
30/07/2018 00:00	1,82
30/07/2018 06:00	1,81
30/07/2018 12:00	1,79
30/07/2018 18:00	1,78
31/07/2018 00:00	1,78
31/07/2018 06:00	1,78
31/07/2018 12:00	1,78
31/07/2018 18:00	1,81
01/08/2018 00:00	1,85

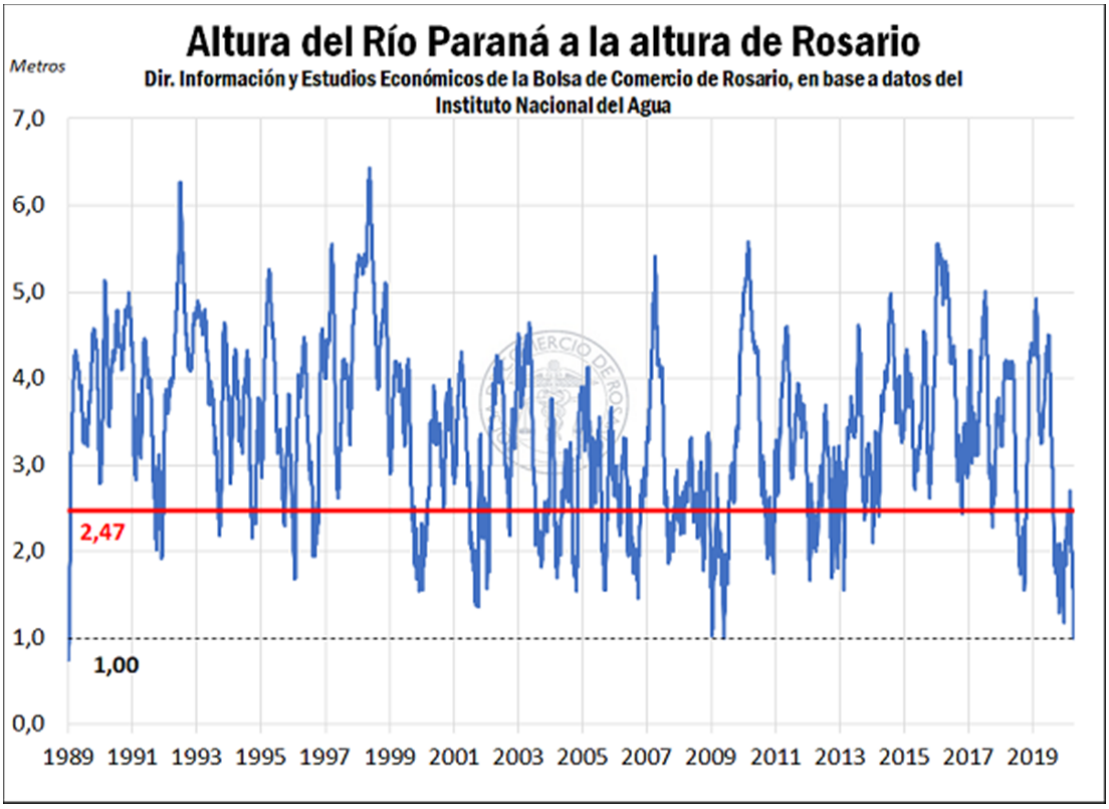
Fuente: Información de histórico de PNA de niveles de Río Paraná en Rosario

Por eso una baja significativa del nivel del Rio Paraná afectará al complejo Gran Rosario desde lo logístico teniendo un impacto económico considerable.

Además el nivel del río Paraná depende de las precipitaciones en Brasil, tal fue el 2018 donde el descenso del nivel fue a causa de un periodo prolongado sin lluvias en el sur de Brasil.

Datos Históricos del Río Paraná en el Puerto de Rosario

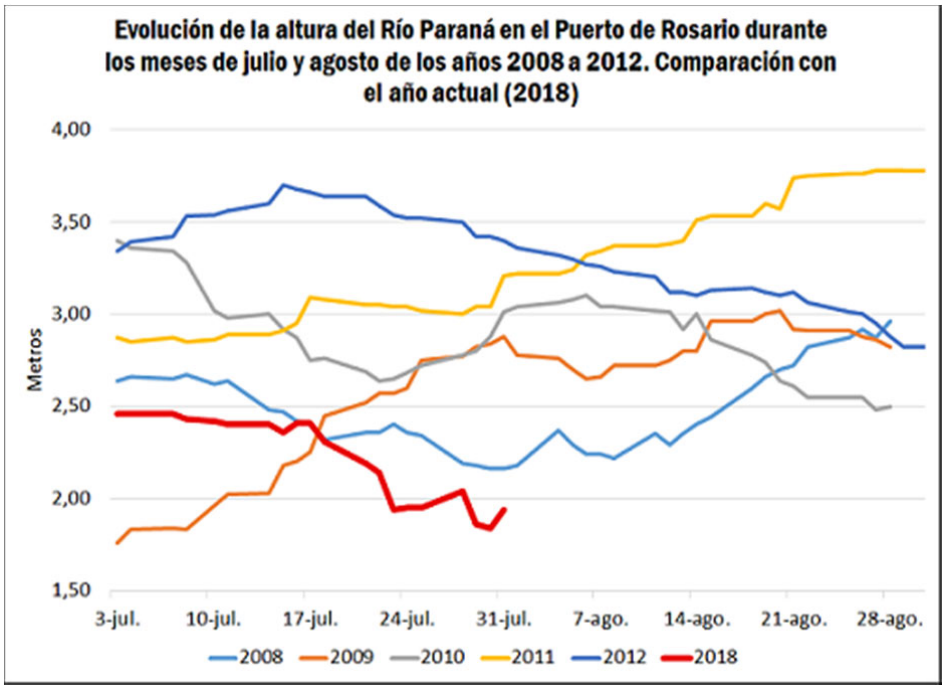
Figura 3.14: Histórico de niveles del río Paraná en Rosario 1989-2019



Fuente: Bolsa de comercio de Rosario Informativo Semanal 8 de Abril 2020

Se pueden comparar los niveles del rio en el Puerto de Rosario desde el año 2008 al 2012 (Figura 3.15) y compararlos al año 2018. Donde se observa significativamente para ese año en el mes de agosto (1,90 metros) supera al más bajo de los registros en el año 2008 en el mismo mes (2,37metros).

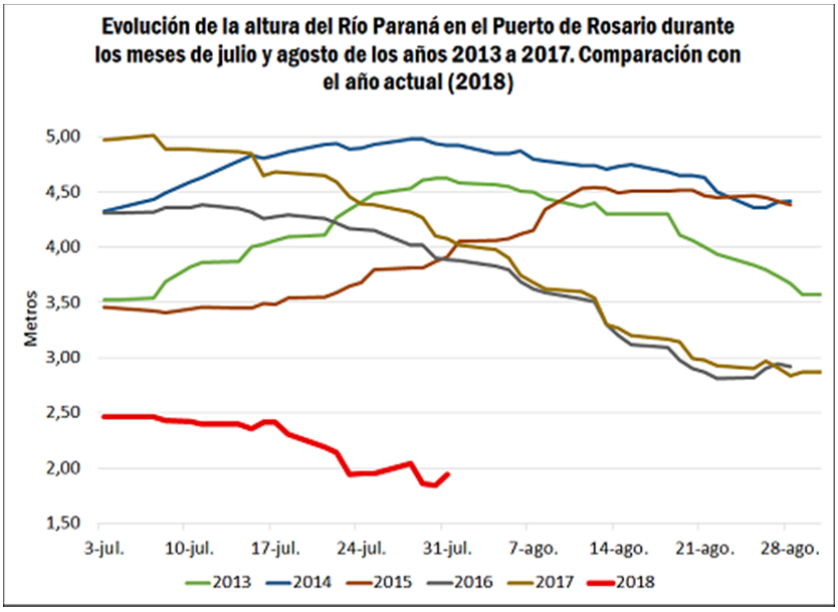
Figura 3.15: Histórico de nivel de ríos de 2008 a 2012



Fuente: Bolsa de comercio de Rosario Informativo Semanal 10 de Agosto 2018

Y el historial desde los años desde el 2013 al 2018 (Figura 3.16) es más pronunciada la diferencia de la baja del rio en agosto 2018 a los años anteriores (2013-2017).

Figura 3.16: Histórico de niveles de ríos 2013 a 2017



Fuente: Bolsa de comercio de Rosario Informativo Semanal 10 de Agosto 2018

Cargas y costos en buques afectados por la bajante

En las operaciones de carga y descarga de los buques se encuentran en la mercadería, harina de soja, maíz, aceite de soja y trigo. Siendo estas las cargas más importantes.

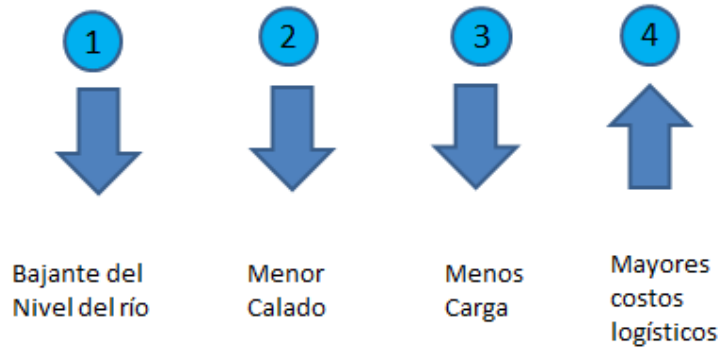
Tal es el caso del 2018, la terminal del puerto de Rosario fue 2 pies menos de profundidad y se tuvo un registro de pérdidas de cargas. Donde los buques más grandes perdieron entre 3.200 y 4.300 tn (Cuadro 3.5). Cuando la profundidad del canal navegable es de 34 pies se tiene la carga óptima en los buques.

Cuadro 3.5: Cantidad de cargas en Buques

Tipos de buques y toneladas que no podrán cargarse en el Gran Rosario por la bajante (Granos y Harinas)				
Tipo de buque	Carga en toneladas en el Gran Rosario		Carga en toneladas en el Gran Rosario	Tonelaje que no podrá cargarse por la bajante
	10,36M	34 PIES	32 pies	
HANDY 20K	19900		19900	0
HANDY 33K	32500		32500	0
SUPRAMAX 50K	38800		35600	3200
SUPRAMAX 56K	39100		35500	3600
PANAMAX 75K	47498		43298	4200
POSTPANAMAX 81K	47850		43500	4350

Fuente: Bolsa de comercio de Rosario Informativo Semanal 10 de Agosto 2018

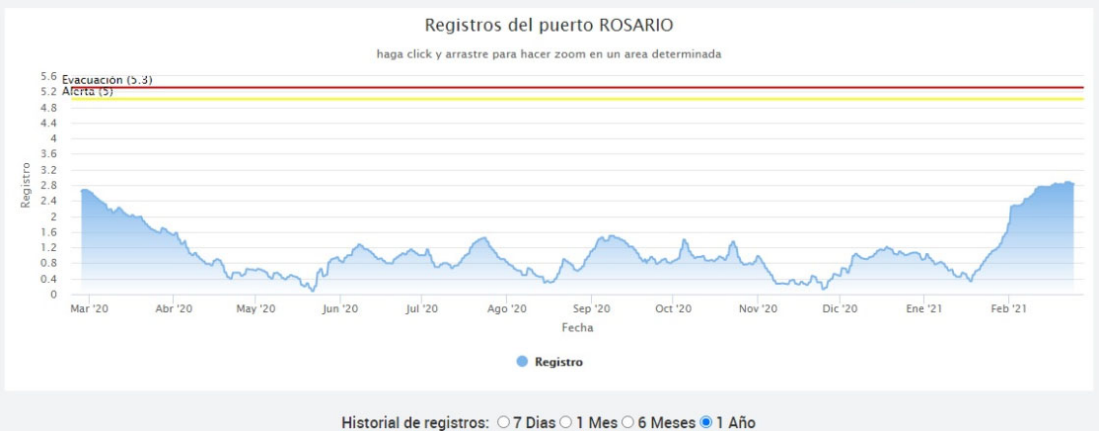
Figura 3.17: Secuencia de impacto ante una bajante de nivel de río



Fuente: Elaboración propia

En Abril del 2020 se registró un nivel de 1 metro en el puerto de Rosario Figura 3.18. Lo cual llevo al uso de dragado para que el calado navegable llegue a 30 pies y poder permitir la navegación de buques cargueros. La disminución del Rio Paraná en ese año representó un costo de u$s244 millones para el complejo agroindustrial.

Figura 3.18: Registro histórico de nivel de Río Paraná de Marzo 2020 a Febrero 2021



Fuente: Sitio contenidosweb.prefecturanaval.gob.ar

Cuadro 3.6: Impacto negativo por la bajante del Río Paraná

Estimación de pérdidas para la República Argentina por la bajante del Río Paraná y su impacto negativo sobre el complejo agroindustrial exportador	
Rubro	**millones de U$S**
Costos de los buques que deben efectuar completamiento en otros puertos y falso flete de los que no pueden completar su capacidad máxima de carga.	91,2
Menores precios de exportación para el aceite de soja argentino por la bajante (baja de las primas FOB argentina en relación a otros orígenes)	86,4
Mayores costos de transporte y logísticos en la mercadería que baja por barcaza desde Paraguay, Brasil y Bolivia	25,2
Demoras de los buques en el proceso de exportación. Cálculo para harina de soja.	13,7
Demoras en la industrialización del complejo oleaginoso del Gran Rosario, ralentización del programa de embarques de maíz, saturación en la capacidad de almacenaje, etc.	27,4
Estimación pérdidas por la Bajante del Río Paraná	**243,9**
Fuente: DIyEE-Bolsa de Comercio de Rosario	

Fuente: Información Noticias Bolsa de Comercio de Rosario 24 de Abril de 2020

Cuadro 3.7: comparación de bajantes críticas de niveles de ríos, afectando las cargas en buques en Rosario

Año	Medida del hidrómetro del Nivel de Río Paraná en el Gran Rosario	Calado o profundidad de canal en el Gran Rosario	Pérdidas de Carga (toneladas) Buques: Handymax y Handysize	Pérdidas de Carga (toneladas) Buques: Supramaxes	Pérdidas de Carga (toneladas) Buques: Panamaxes, Postpanamaxes y Kamsarmaxes	Total de Carga perdida (toneladas)
2018	1,86m	32 pies	3000 a 3600	3200 a 3600	4000 a 5000	10200 a 12200
2020	1,27m	30 pies	4500 a 5400	4800 a 5400	6000 a 7500	15300 a 18300

Fuente: Elaboración propia en base a la información de la Bolsa de Comercio de Rosario

Entonces hay una necesidad de ajustar el volumen de carga cada vez que se tiene menor nivel del rio. Existen diferentes buques con distintas capacidades de carga, entre ellos los más importante son:

- Handysize o Handimax con una capacidad de carga de 35000 y 40000 toneladas. Y la baja del rio en 1 pie esto representa una pérdida de carga entre 1500 y 1800 toneladas.
- Luego siguen los buques de tamaño intermedio llamados Supramaxes con capacidad de carga de 50000 y 60000 toneladas y de perder dos pies de profundidad representa una pérdida de carga entre 3200 y 3600 toneladas.
- Por ultimo están los buques grandes Panamaxes, Postpanamaxes y Kamsarmaxes con capacidad entre 60000/65000 y 90000 toneladas. En estos por cada pie menos ,pierden entre 2000 y 2500 toneladas de carga.

Cuadro 3.8: Cargas perdidas por pies de calado de canal

Pies de calado o profundidad de canal navegable en Rosario	Pérdidas de Carga (toneladas) Buques: Handymax y Handysize	Pérdidas de Carga (toneladas) Buques: Supramaxes	Pérdidas de Carga (toneladas) Buques: Panamaxes,Postpanamaxes y Kamsarmaxes
34	0	0	0
33	1500 a 1800	1600 a 1800	2000 a 2500
32	3000 a 3600	3200 a 3600	4000 a 5000
31	4500 a 5400	4800 a 5400	6000 a 7500
30	6000 a 7200	6400 a 7200	8000 a 10000

Fuente: Elaboración propia en base a la información de la Bolsa de Comercio de Rosario

Otros impactos a tomar en cuenta son los costos logísticos, transporte, industrialización y operativos debido a las pérdidas de cargas en puerto por la bajante del Río Paraná. Existen los costos de buques de gran porte en relación de la necesidad de ajuste de volumen de carga en Puerto Gran Rosario y realizar el completamiento en otros puertos de la zona. Y por otro lado están los costos de buques de menor porte, estos incurren en un falso flete por no poder completar su capacidad máxima de carga.

Buques de gran porte

Entonces si antes los buques de mayor porte como Panamax cargaban con 45000 toneladas de cereal y completaban la carga en Bahía Blanca hasta 60000 toneladas, están obligados a salir del Puerto Gran Rosario con menos carga por la falta de profundidad. Y obliga a estos buques de gran porte a cargar más maíz en puertos del sur bonaerense, habiendo problemas de logística debido a la existencia de menor disponibilidad de cereal en el sur bonaerense y los costos de adquisición son más elevados.

En muchos casos hay una retribución adicional a los productores por el mayor coste de flete de trasladar granos ubicados más alejados de puertos bonaerenses. Los mayores costos de transporte, adquisición y logísticos se estiman en 25 U$S por cada tonelada que no se pudo cargar en el Gran Rosario. Pasa lo mismo con el poroto de soja. Donde afectan más con los buques supramax y panamax graneleros.

Para el caso de un buque Panamax con una capacidad de carga entre 60000 a 65000 toneladas, la pérdida de 4 pies de calado o profundidad en el Gran Rosario tiene como consecuencia en el buque la perdida de cargar entre 8000 y 10000 toneladas por buque. Si se cargan harinas, la perdida puede ser menor porque pesa menos por volumen de carga.

Buques de menor porte

Los buques de menor porte como Handysize o Handymax pierden cargas entre 1500 y 1800 toneladas por cada pie de calado que baja el río Paraná. Al tratarse de menor tamaños estos buques, no realizarán completamiento en Bahía Blanca o Quequén. Esto se lo

denomina el costo Falso Flete porque el transporte al exterior cuesta lo mismo pero llevan menos mercadería por la bajante del río.

Tomando el ejemplo del costo de viaje de un buque Handymax con graneles secos agrícolas, de Gran Rosario a Medio Oriente serían unos U$S 1.027.000. A partir del cual se puede calcular el aumento del costo por tonelada transportada debido a la menor utilización de capacidad de carga y el viaje es directo de origen a destino sin realizar el completamiento de carga.

Entonces el costo de viaje a Medio Oriente de un Handymax: U$S 1.027.000

A la profundidad de 34 pies en el Gran Rosario la carga en el Handymax es de 40.000 toneladas por lo que el costo de flete es de 26U$S por tonelada.Y en el caso de tener 30 pies de profundidad en el Gran Rosario el Handy va cargar menos con un valor de carga de 33.192 toneladas y el costo de flete es de 31U$S por tonelada.

Siendo el falso flete con un costo de U$S164.000 por cada buque (esto es el producto de igual costo de transporte en el viaje más cargado versus el mismo costo de viaje con menos carga, es decir la diferencia de mayor costo unitario por las toneladas que efectivamente se transporta).

Cuadro 3.9: Costos por las cargas perdidas por pies de canal

Pies de calado o profundidad de canal en Rosario	Costos por Pérdidas de Carga (U$S) Buques: Handymax y Handysize	Costos por Pérdidas de Carga (U$S) Buques: Supramaxes	Costos por Pérdidas de Carga (U$S) Buques: Panamaxes,Postpanamaxes y Kamsarmaxes
34	0	0	0
33	26000 a 33800	40000 a 45000	50000 a 62500
32	65000 a 80600	80000 a 90000	100000 a 125000
31	104000 a 127400	120000 a 135000	150000 a 187500
30	143000 a 164000	160000 a 180000	200000 a 250000

Fuente: Elaboración propia en base a la información de la Bolsa de Comercio de Rosario

Barcazas

Aumento de costos logísticos y de transporte de mercadería que baja por Hidrovía Parana-Paraguay, es decir desde países limítrofes a los puertos del Gran Rosario, para la importación temporaria por su posterior procesamiento y exportación o para trasbordo en los puertos del Gran Rosario.

A nivel logístico es muy importante el ingreso de soja que ingresa año a año desde Bolivia, Brasil y Paraguay, para luego exportarse en buques de mayor porte en las terminales del Gran Rosario. Y en el en caso de soja que ingresa de Paraguay es muy importante para la industria local y el complejo oleaginoso del Gran Rosario porque se mezcla con poroto de soja de origen argentino ayudando a elevar el nivel de proteína de la harina de soja y así cumplir con las exigencias de la demanda internacional.

Ante la bajante del Río trae consecuencias de la llegada de barcazas de Paraguay con soja pudiendo llegar al Complejo Industrial Oleaginoso del Gran Rosario con demoras de entre 10 a 15 días. Esto trae retrasos en la industrialización del poroto en el Gran Rosario y los incumplimientos de programa de embarques y contratos de compra en el exterior.

Lo más importante es que se requieren mayores barcazas (de Bolivia ,Brasil y Paraguay) para bajar la misma mercadería al Gran Rosario debido a la bajante del rio. Y entonces se genera un importante aumento en costos de transporte para las empresas del sector.
En el costo de transporte de las barcazas con un nivel óptimo de las aguas en la Hidrovía Paraná – Paraguay, las barcazas bajan normalmente desde Paraguay con 10 pies de calado o profundidad y en trenes de 6 por 7 barcazas, siendo este un total de 42 barcazas. Y cada barcaza transporta 1.500 toneladas, siendo la carga total por tren de barcazas oscilando en 63.000 toneladas.

Por la bajante del rio a 6 pies de profundidad, cada barcaza transporta individualmente alrededor de los 900 toneladas y el tren de barcazas se reduce a 6 por 5 , implicando 30 barcazas por cada tren. Siendo 27000 toneladas en total lo que transporta cada tren de barcazas. Se necesitaría el doble el doble de barcazas para traer la misma carga (que en condiciones normales de 10 pies de profundidad) desde Paraguay al Gran Rosario.

Entre otros impactos están:

- Las demoras en el proceso de exportación. La baja del rio obliga a prácticos y pilotos a tener mayor prudencia y en especial en canales de acceso y pasos críticos ya que existe la posibilidad que se registre varaduras en el rio con posibilidad de afectar la óptima navegación. Y el costo por cada día de demora de un buque para cargar y despachar al exterior es de U$S 45000.
- Las demoras en la carga de buques con aceite de soja afectando el ritmo de exportación de harina.
- Las demoras en la industrialización del complejo oleaginoso de Gran Rosario con la posibilidad de ralentización del programa de embarques de maíz entre los meses de Abril y Mayo, donde podría darse problemas de saturación en la capacidad de almacenaje del grano en los puertos. Demoras de importancia en la carga de buques con aceite de soja generando inconvenientes en fábricas, demoras en el ritmo de molienda y saturación de almacenamiento.
- Debido a los retrasos en ingreso de mercadería del exterior como el cuello de botella de ralentización de embarques y otros factores mencionados anteriormente tiene un costo estimado de U$S 3 por tonelada procesada.
- Medioambiente, Represa, pesqueros y practicaje deportivo.

3.3.5 Problema de un registro centralizado

El registro centralizado tiene la desventaja de que un ataque a un nodo central critico como es el caso de registro de altura de ríos pondría en riesgo a toda la estructura. Los sistemas centralizados pueden ser hackeados o sufrir suplantación de identidad, como el caso de ataque en el registro en un mismo lugar físico o virtual.

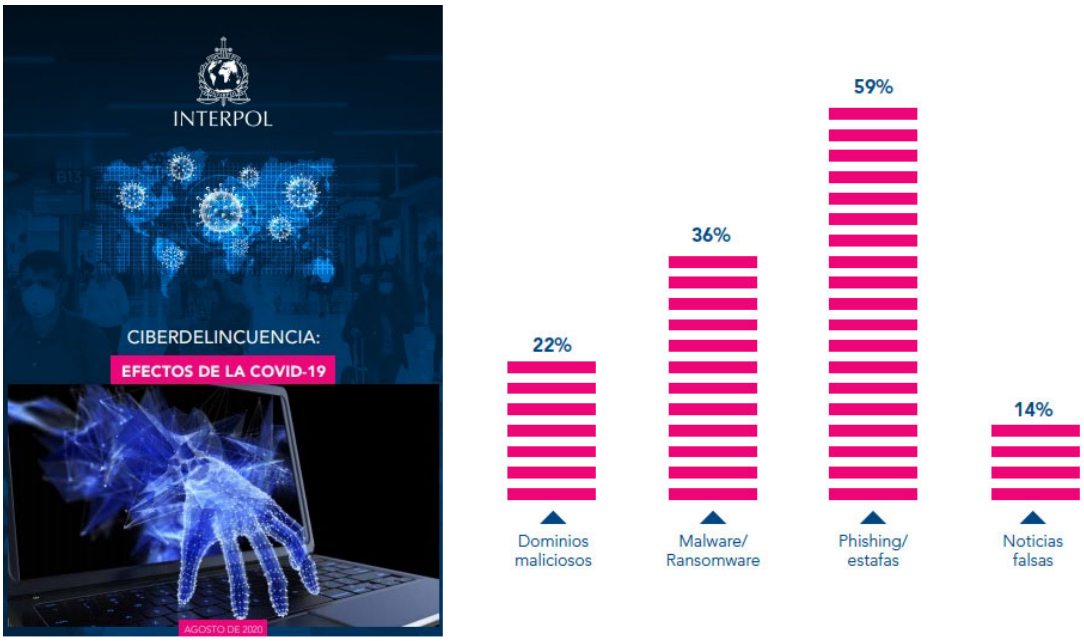
Los tipos de ataques a un sistema de información centralizado pueden ser realizados a una web mediante técnicas conocidas como inyección de códigos para lograr tener acceso al servidor o sistema corrompiendo los datos. También los ataques al sistema pueden ser mediante técnicas de Phising y Malware para manipular los datos.

Un informe de *INTERPOL* en el escenario de pandemia muestra un aumento de ciberataques. La ciberdelincuencia cambió sustancialmente en los objetivos de ataques que

eran antes particulares y pequeñas empresas, ahora la tendencia es a las grandes multinacionales, administraciones estatales e infraestructuras esenciales.

La dependencia de internet es notable en este escenario. Hay un aumento de conectividad de usuarios en esta pandemia, donde también las organizaciones y las empresas han desplegado en forma rápida redes y sistemas en forma remota para el personal. Los delincuentes aprovecharon el aumento de vulnerabilidades en seguridad informática para robar datos y ocasionar disfunciones.

Figura 3.19: Ciberamenazas detectadas durante el año 2020



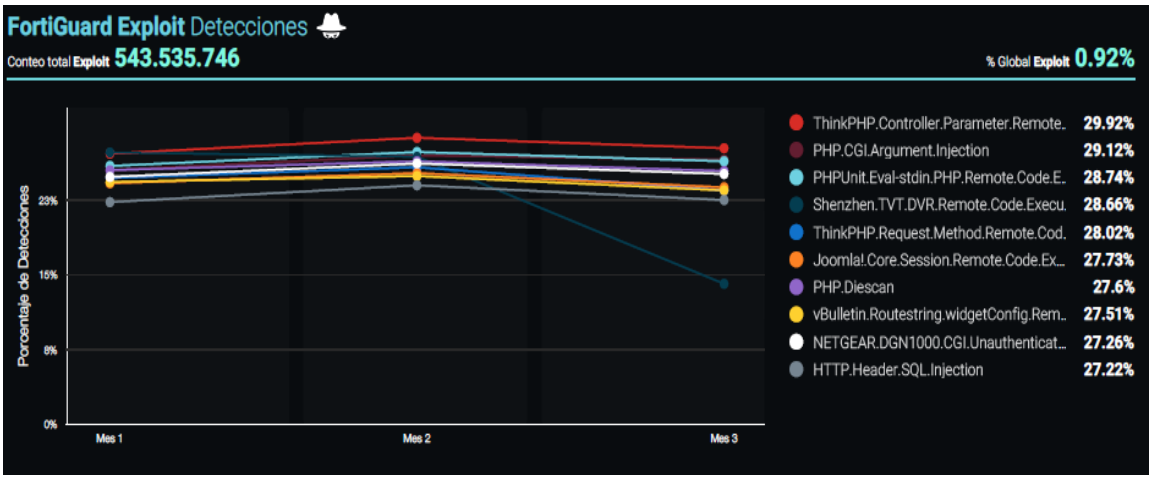
Fuente: Reporte de Interpol Agosto 2020

El jefe de INTERPOL concluye la necesidad de una cooperación más estrecha entre los sectores público y privado para atajar con eficacia el peligro a la salud cibernética.

Se pueden observar los distintos intentos de explotar una vulnerabilidad en la Figura 3.20 a través de un reporte del 2020 informado por la empresa de equipos *Fortinet* (una de las empresas líderes en equipos *Firewall*). Los ataques observados son intentos de explotar o encontrar una vulnerabilidad de ejecución remota de código de un marco web conocido como *ThinkPHP* y *PHPUnit* (usados por una gran cantidad de desarrolladores web). La

vulnerabilidad se reveló en el año 2018, una falla que permite a los atacantes remotos la ejecución de un código arbitrario que podría permitir al atacante el acceso a un servidor vulnerable y luego instalar software malicioso (conocido como *malware*).

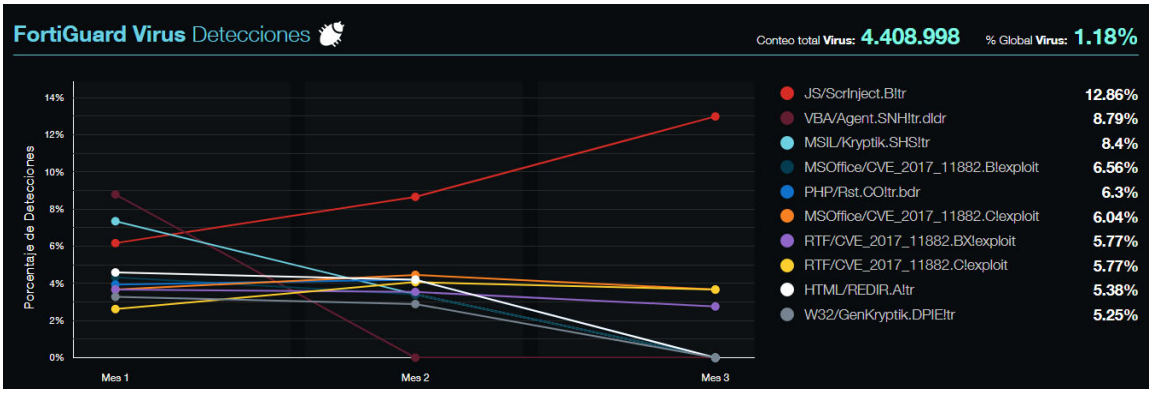
Figura 3.20: Ataques detectadas a web en ARGENTINA en el año 2020



Fuente: Boletín informativo de amenazas *Fortinet Threat Intelligence Insider 2020*

El software malicioso es llamado *Malware* y estos pueden ser conocidos como basados en web, llamados *phising*, estos se van extendiendo por América Latina e intentan redirigir el navegador web a un sitio para el inicio de una intrusión. El malware en la web se ha convertido en el medio más común para la distribución de archivos maliciosos. También se detectaron numerosos campañas de troyanos durante el 2020 , estos realizan actividades sin conocimiento del usuario ,incluyen establecimiento remoto , realizando la captura de entrada de teclado , la recopilación de la información del sistema, la carga y descarga de archivos y la colocación de software malicioso en el sistema, se ejecutan denegaciones de servicio y ejecutan o eliminan procesos. El tipo de malware más activo durante el 2020 fue el llamado *JS/ScrInject.B! (troyano)* tal como se observa en la Figura 3.21.

Figura 3.21: Ataques detectadas de virus troyanos en ARGENTINA en el año 2020



Fuente: *Boletín informativo de amenazas Fortinet Threat Intelligence Insider 2020*

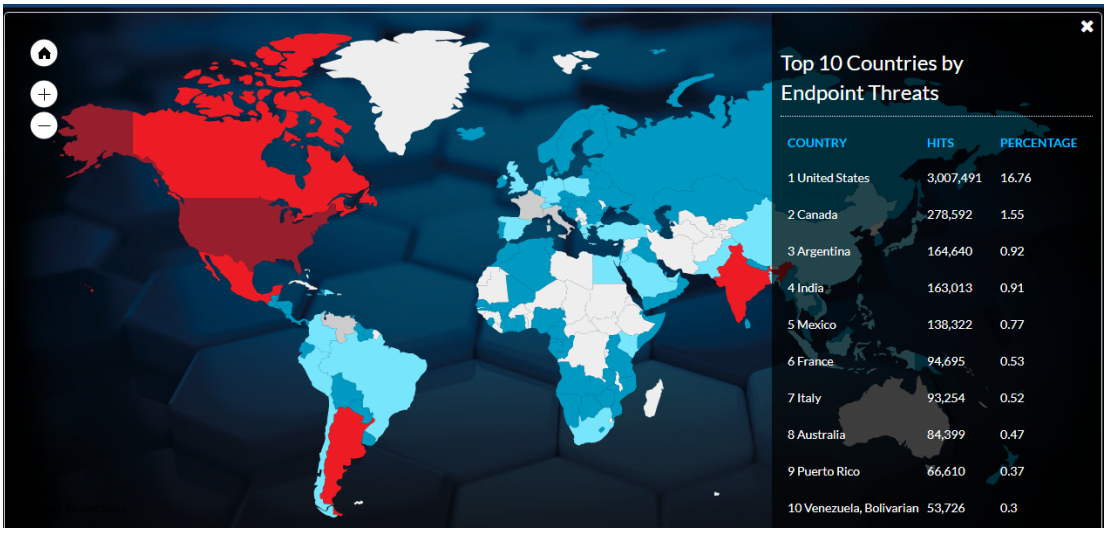
Otros informes de la empresa Fortinet son a través de mapas de amenazas *Fortiguard Labs* de su sitio como se observa en la Figura 3.22, donde Argentina en la actualidad se encuentra entre los países con más amenazas de virus en el mundo siendo el tercer país del top 10.

Figura 3.22: Informe diario mundial de amenazas de virus Top 10

Fuente: Sitio *fortiguard.com*

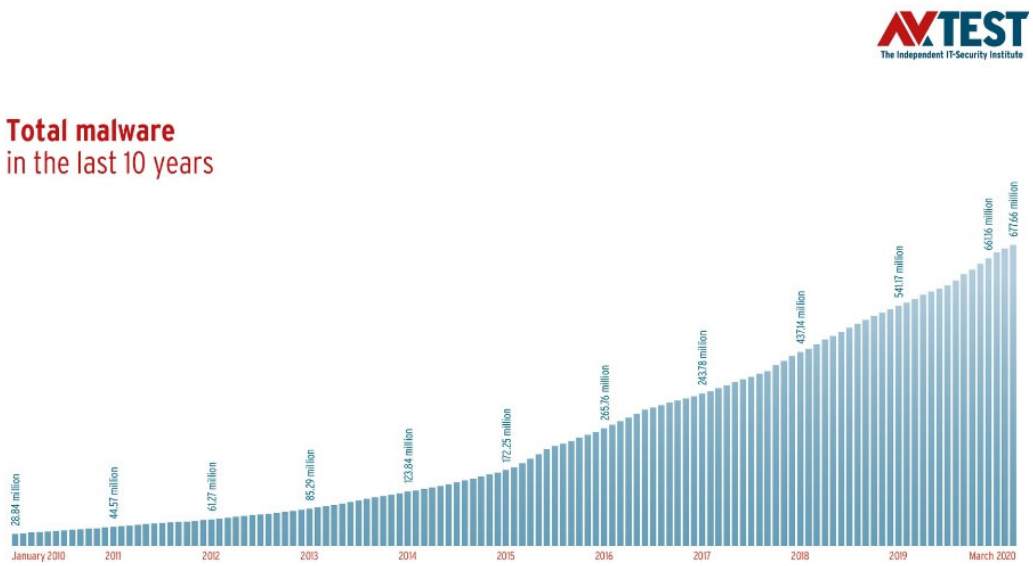
Y también está el mapa de amenazas a las organizaciones, donde Argentina se encuentra en la posición tercera Figura 3.23:

Figura 3.23: Figura: Informe diario mundial de amenazas a Infraestructuras Top 10



Fuente: Sitio *fortiguard.com*

Figura 3.24: Evolución global de malware



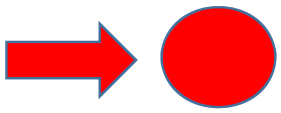
Fuente: Sitio *av-test.org*

Entonces los riesgos de un ciberataque son latentes y las consecuencias de una manipulación en el registro centralizado de altura de ríos harían que la Prefectura Naval Argentina divulgue a través de la web una mala información de niveles de ríos y así no sea confiable ni de garantía la información publicada en la web. Y los registros históricos de altura de ríos modificados dan lugar a malas interpretaciones:

- Malos pronósticos de alturas de ríos.
- Falsos niveles de altura de ríos afectan a las cargas de mercadería en buques y barcazas.
- Costos elevados de las operaciones de transporte.
- Mala información para represas,ribereños, pesqueros y practicaje deportivo.

Un escenario puede ser una modificación del valor de altura de río con un valor menor al valor real medido, tal como puede observarse en la siguiente Figura 3.25.

Figura 3.25: Ataque a un sistema centralizado



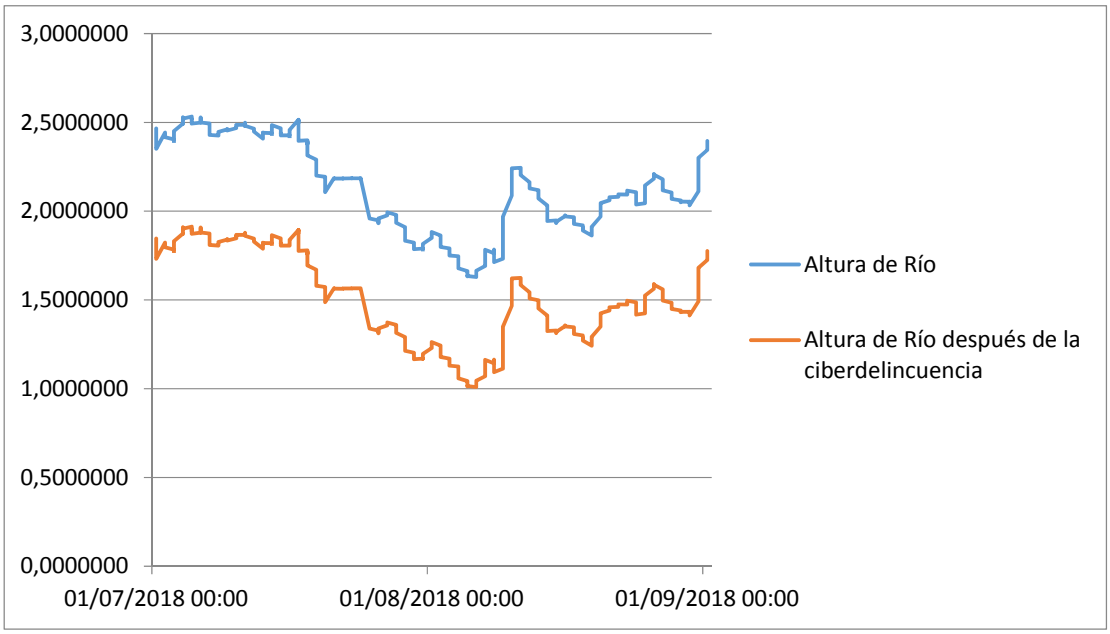
	Antes del ataque	Después del ataque
Nivel del Río Paraná	2,47m	1,85m

Fuente: Elaboración propia

Y la modificación da lugar a un mal pronóstico (a 6 días) y tendencia (a 16 días) del nivel de río en base a las lecturas manipuladas en el registro de altura. Es decir un ataque de ciberdelincuencia afecta los valores de registro de altura por lo que como consecuencia se tiene una mala interpretación y provocaría cambios en los pronósticos para los próximos días y en esa mala lectura por el ataque, se interpretaría como consecuencia, ajuste de carga y costos en buque y barcazas en la Hidrovía Paraná-Paraguay. El INA toma las lecturas de PNA para realizar el informe de pronósticos. La altura de río en el puerto de Rosario depende de las precipitaciones ocurridas en cuencas como en Brasil y si las lluvias comenzaran a darse en crecimiento gradual pero los valores que se midan en el día fuesen modificados entonces no reflejaría una tendencia y pronósticos favorables de navegación.

Otro escenario, de producirse un ciberataque y se esté manipulándose el historial correspondiente al 2018 con valores 0,3048 m (1 pie) menos del nivel de rio, se tendría entonces la modificación como se observa en la Figura 3.26. Es decir como consecuencia es una mala interpretación del estado de navegación y el impacto es menos carga en los buques y mayores costos de logística y transporte (Cuadro 3.10).

Figura 3.26: Cambio de valores en el Historial ante una manipulación de decremento de altura de río



Fuente: Elaboración propia en base a los datos históricos de registro de niveles del 2018

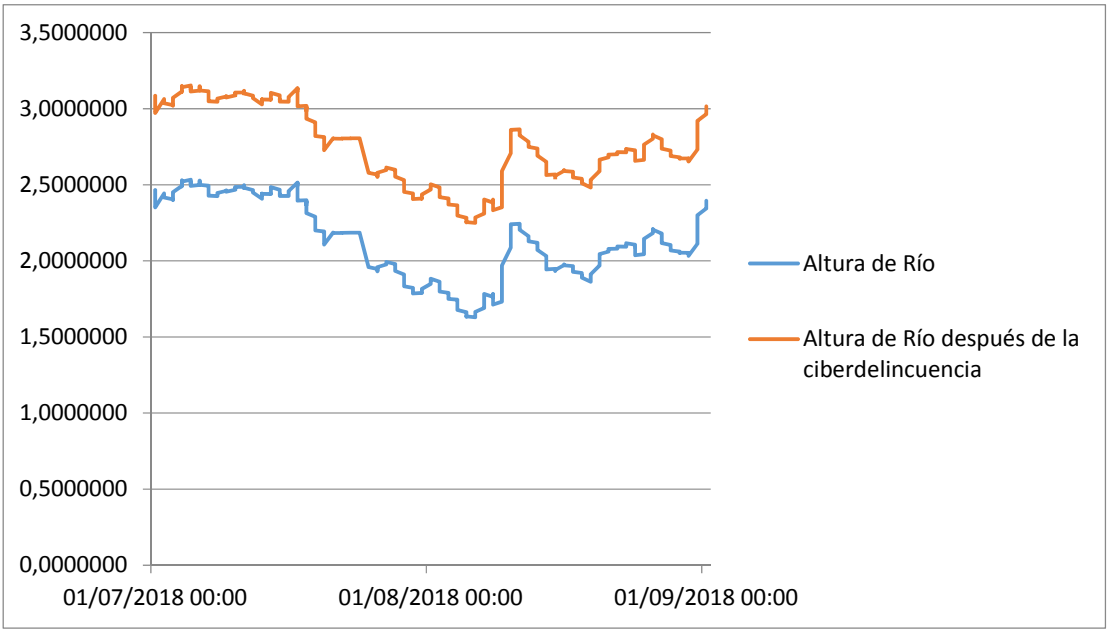
Cuadro 3.10: Riesgos de manipulación de decremento de nivel de río

Buques	Cargas perdidas (toneladas) y Costos (U$S) **antes del ciberataque**	Cargas perdidas (toneladas) y Costos (U$S) **después del ciberataque**
Handymax y Handysize	Cargas: 3000 a 3600 Costos: 65000 a 80600	Cargas: 4500 a 5400 Costos: 104000 a 127400
Supramaxes	Cargas: 3200 a 3600 Costos: 80000 a 90000	Cargas: 4800 a 5400 Costos: 120000 a 135000
Panamaxes,Postpanamaxes y Kamsarmaxes	Cargas: 4000 a 5000 Costos: 100000 a 125000	Cargas: 6000 a 7500 Costos: 150000 a 187500

Fuente: Elaboración propia

O de darse el caso en el ciberataque en el que se modifique los valores del historial del año 2018 con un valor mayor al real Figura 3.27, teniendo el riesgo de interpretación que se confirme la seguridad de navegación de buques cargando más mercadería confiando en la garantía de la información. Donde indicaría poder cargar más mercadería en los buques y menos serían los costos de logística y transporte (Cuadro 3.11).

Figura 3.27: Cambio de valores en el Historial ante una manipulación de incremento de altura de río



Fuente: Elaboración propia en base a los datos históricos de registro de niveles del 2018

Cuadro 3.11: Riesgos de manipulación de incremento de nivel de río

Buques	Cargas perdidas (toneladas) y Costos (U$S) antes del ciberataque	Cargas perdidas (toneladas) y Costos (U$S) después del ciberataque
Handymax y Handysize	Cargas: 3000 a 3600 Costos: 65000 a 80600	Cargas: 1500 a 1800 Costos: 26000 a 33800
Buques Supramaxes	Cargas: 3200 a 3600 Costos: 80000 a 90000	Cargas: 1600 a 1800 Costos: 40000 a 45000
Buques Panamaxes,Postpanamaxes y Kamsarmaxes	Cargas: 4000 a 5000 Costos: 100000 a 125000	Cargas: 2000 a 2500 Costos: 50000 a 62500

Fuente: Elaboración propia

O si es un escenario de caso extremo donde puede manipularse el valor de nivel de rio llevando a una altura de 1m,dando una mala interpretación de un falso dragado y gran costo logístico con muchas pérdidas de cargas en buques y altas pérdidas en U$S (Cuadro 3.12). Repitiendo lo sucedido en el año 2020.

Cuadro 3.12: Consecuencias ante una manipulación de 4 pies

Manipulación del Nivel de registro de Río en el Gran Rosario	Total de Carga perdida (toneladas)	Pérdidas en U$S
1,25m	**18300**	**594000**

Fuente: Elaboración propia

De no contar con Blockchain y estar usando un registro centralizado se tiene el riesgo de una manipulación y modificación de los niveles históricos de ríos, dando lugar a malas interpretaciones de impacto en los costos y las cargas de buques y barcazas de las actividades del Gran Rosario. Considerando que es un complejo agroindustrial importante para la economía de la República Argentina. A continuación se muestran los riesgos de una mala interpretación de no aplicar Blockchain:

Cuadro 3.13: Consecuencias en un ataque con registro centralizado sin blockchain

Manipulación del Nivel de registro de río en el Gran Rosario	Buques	Sin Blockchain Cargas(toneladas) perdidas y Costos(U$S)	Con Blockchain Cargas(toneladas) perdidas y Costos(U$S)
↓2,16 m	Handymax y Handysize	carga = 1500 a 1800 costo = 26000 a 33800	carga = 0 costo = 0
	Supramaxes	carga = 1600 a 1800 costo = 40000 a 45000	carga = 0 costo = 0
	Panamaxes,Postpanamaxes y Kamsarmaxes	carga = 2000 a 2500 costo = 50000 a 62500	carga = 0 costo = 0
↓1,86 m	Handymax y Handysize	carga = 3000 a 3600 costo = 65000 a 80600	carga = 0 costo = 0
	Supramaxes	carga = 3200 a 3600 costo = 80000 a 90000	carga = 0 costo = 0
	Panamaxes,Postpanamaxes y Kamsarmaxes	carga = 4000 a 5000 costo = 100000 a 125000	carga = 0 costo = 0
↓1,55 m	Handymax y Handysize	carga = 4500 a 5400 costo = 104000 a 127400	carga = 0 costo = 0
	Supramaxes	carga = 4800 a 5400 costo = 120000 a 135000	carga = 0 costo = 0
	Panamaxes,Postpanamaxes y Kamsarmaxes	carga = 6000 a 7500 costo = 150000 a 187500	carga = 0 costo = 0
↓1,25 m	Handymax y Handysize	carga = 6000 a 7200 costo = 143000 a 164000	carga = 0 costo = 0
	Supramaxes	carga = 6400 a 7200 costo = 160000 a 180000	carga = 0 costo = 0
	Panamaxes,Postpanamaxes y Kamsarmaxes	carga = 8000 a 10000 costo = 200000 a 250000	carga = 0 costo = 0
		Mayor Carga perdida y Mayor Costo por cada pie menos de profundidad	Se detecta manipulación con Blockchain, se evitan riesgos

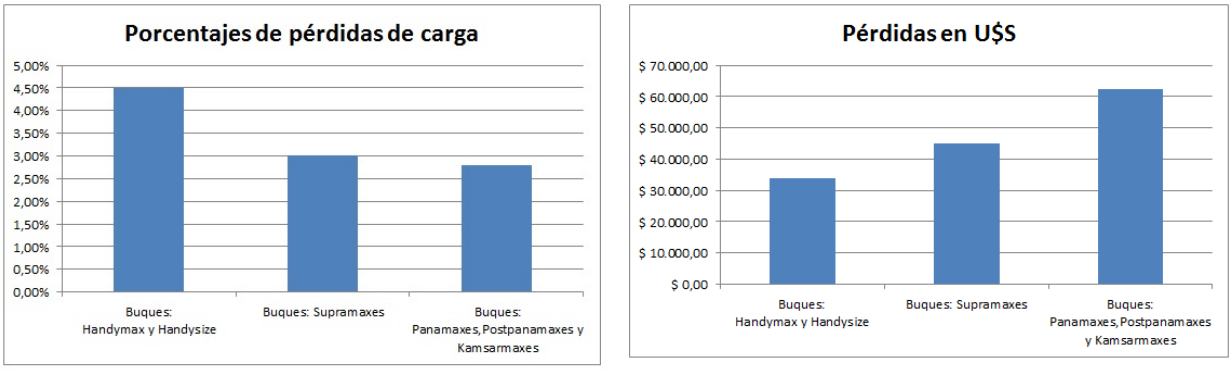
Fuente: Elaboración propia

Cuadro 3.14: Riesgos ante una manipulación del nivel de río

Manipulación del Nivel de registro de río en el Gran Rosario	Porcentaje de Carga perdida Buques: Handymax y Handysize	Porcentaje de Carga perdida Buques: Supramaxes	Porcentaje de Carga perdida Buques: Panamaxes,Postpanamaxes y Kamsarmaxes	Total de Cargas perdidas en porcentaje
↓2,16 m (1 pie menos)	4,50%	3%	2,80%	**10,30%**
↓1,86 m (2 pies menos)	9%	6%	5,60%	**20,60%**
↓1,55 m (3 pies menos)	13,50%	9%	8,40%	**30,90%**
↓1,25 m (4 pies menos)	18%	12%	11,20%	**41,20%**

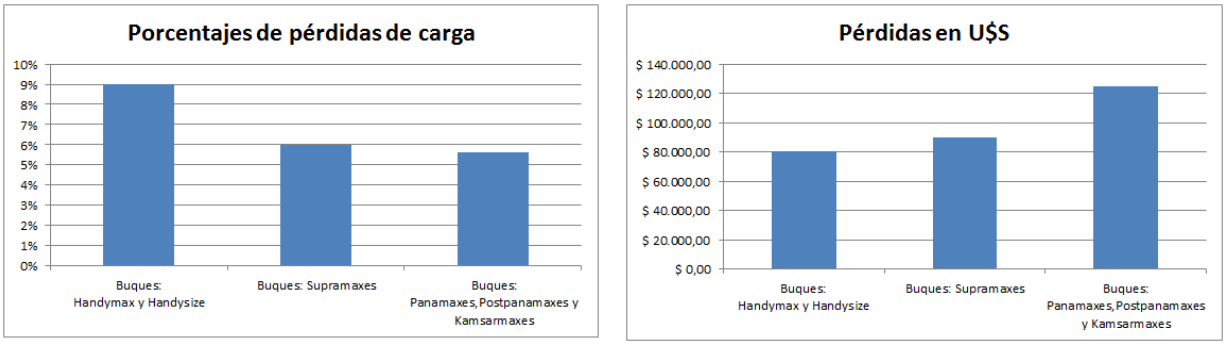
Fuente: Elaboración propia

Figura 3.28: Riesgos de una manipulación de 1 pie menos de nivel de río



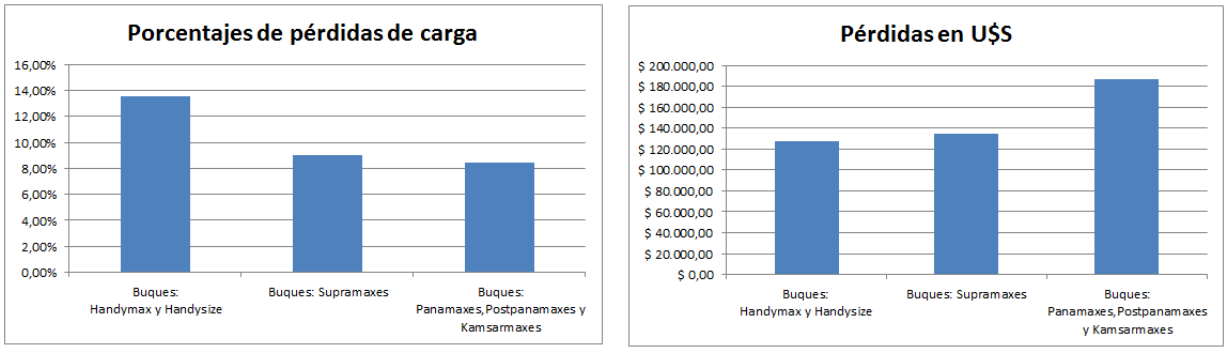
Fuente: Elaboración propia

Figura 3.29: Riesgos de una manipulación de 2 pies menos de nivel de río



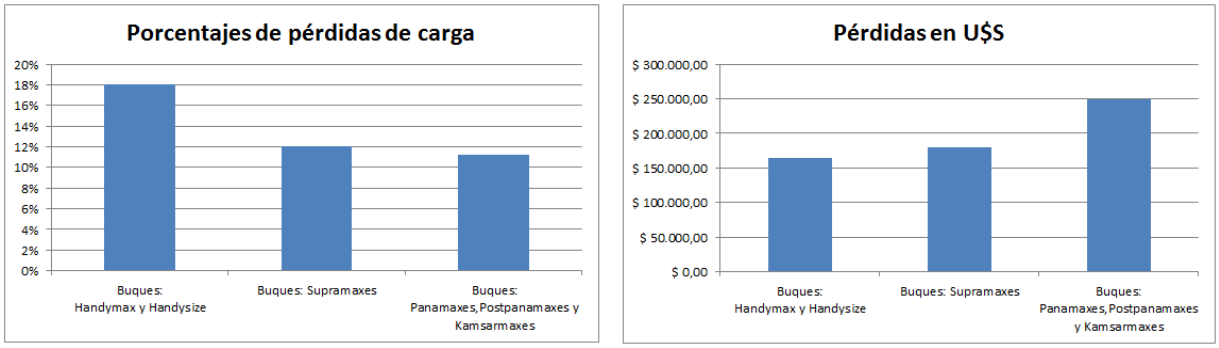
Fuente: Elaboración propia

Figura 3.30: Riesgos de una manipulación de 3 pies menos de nivel de río



Fuente: Elaboración propia

Figura 3.31: Riesgos de una manipulación de 4 pies menos de nivel de río



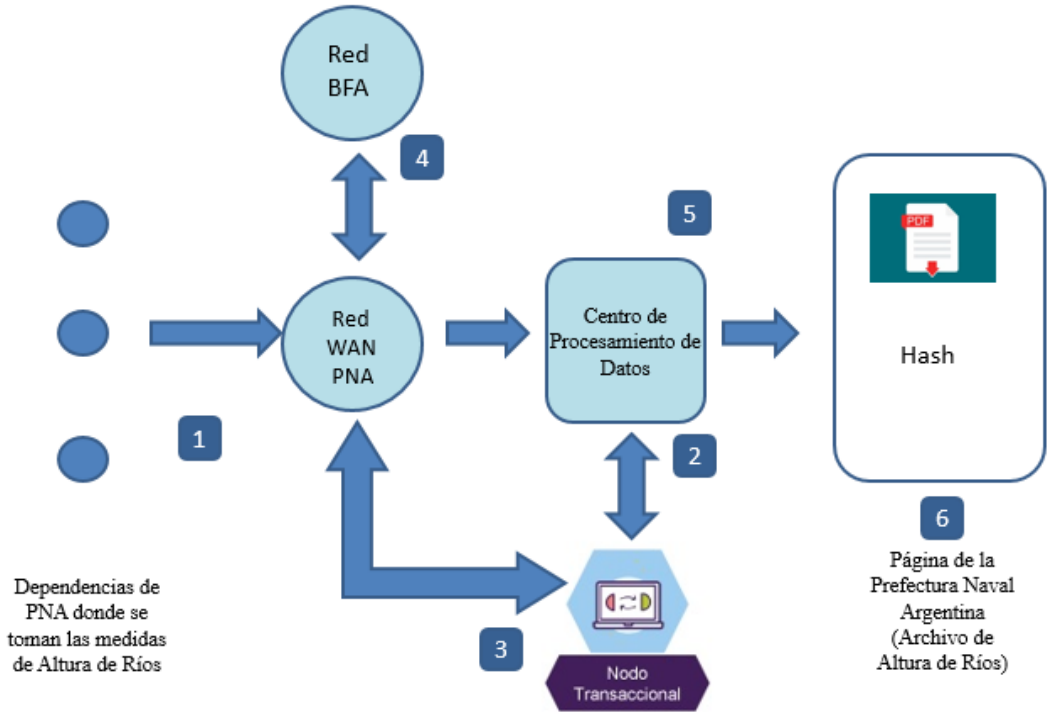
Fuerte: Elaboración propia

3.3.6 Aplicación de Blockchain al Registro de Altura de Ríos

Y como iniciativa y forma de prevención, la idea fue registrar los archivos pdf (registro de las mediciones de niveles de ríos) en la BFA y así aprovechar las características que brinda la tecnología *Blockchain*, dándole a esta información publicada en la web PNA el valor agregado como es la Confiabilidad en la Institución, Garantía de la publicación y así el usuario o navegante pueda consultar a través de un comprobante, que la información de los registros (pdf) es inmutable. A continuación se explica el proceso.

Proceso de aplicación de *Blockchain* al registro de Altura de Ríos:

Figura 3.32: Aplicación de *Blockchain* al proceso



Fuente: Elaboración propia

1) Desde distintas dependencias se toman las medidas de altura de Ríos en forma diaria. Y se envían mediante Internet y llega a la Red PNA (Prefectura Naval Argentina) del Edificio Guardacostas.

2) En el Edificio Guardacostas en el sector de procesamiento de datos se juntan todos los documentos de altura de Ríos y se digitaliza en un archivo pdf con todas las medidas. Se ejecuta un *Script* que va realizar todas las secuencias que vienen a continuación. Se aplica Hash al documento pdf.

3) Luego se envía el Hash a la aplicación *Blockchain* para registrar a través del nodo transaccional.

4) El nodo transaccional llama al *Smart Contract* (este está desplegado en la Red BFA) para realizar el registro del archivo pdf. Una vez registrado en la BFA, el *Smart Contract* devuelve el certificado correspondiente al documento pdf.

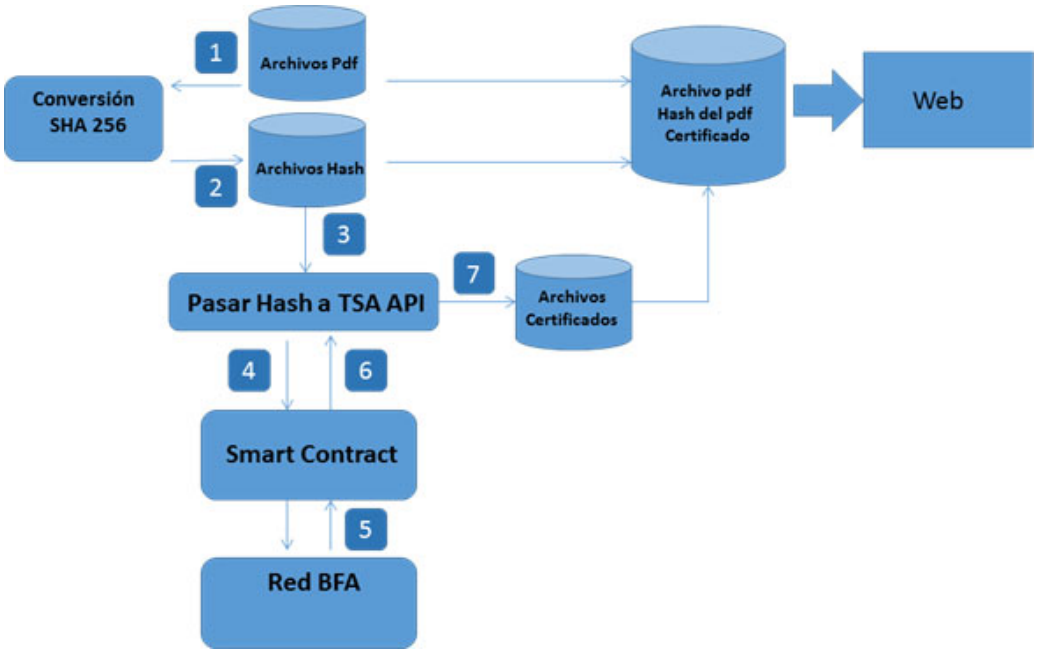
5) El certificado de registro es devuelto al Centro de Datos del Edificio Guardacostas.

6) Finalmente se publican: archivo pdf junto al Hash y al certificado de registro.

Funcionamiento en detalle del *Script*:

Para el proceso de certificar en *Blockchain* se realizó un *script Bash* en *Ubuntu* que comprende la siguiente secuencia:

Figura 3.33: Proceso de *Script*



Fuente: Elaboración propia

1) Se envia el archivo *pdf* de Altura de Ríos a la función *Hash*.

2) Se realiza la conversión *SHA 256* , obteniendo así el archivo hash y se lo almacena.

3) El hash se inserta en la aplicación la *Tsa Api*.

4) La *TSA Api* dialoga con el *Smart Contract* de *Proof of Existence*, ejecutando la función de insertar el *hash* en un bloque de la BFA.

5) El *Smart Contract* inserta el *Hash* en un bloque de BFA.

6) Una vez insertado el *Hash* en la BFA, se devuelve el número de bloque a través de la función del *Smart Contract*.

7) La *TSA Api* toma la devolución del *Smart Contract* y genera un archivo como certificado de registro y se almacena.

8) Se logra así obtener los 3 archivos almacenados y se muestran en el sitio web Figura 3.33 de Altura de Ríos: archivo *pdf , hash* y el certificado en *Blockchain.*

Figura 3.34: Sitio web de certificados *Blockchain*

Fuente: Sito de aplicación de Altura de Ríos

En la Figura 3.34 anterior se puede ver la *web* (creado en *php*) donde se muestran por fecha y hora , los archivos pdf, *hash* y su comprobante de registro en la BFA.

Los resultados con esta aplicación permiten a la PNA ser una de las primeras autoridades marítimas en aplicar *Blockchain* con un entorno de desarrollo de trabajo para seguir desplegando *Smart Contracts.*

A comparación de un registro centralizado, con *Blockchain* se tienen ventajas tal como puede observarse en el Cuadro 3.15.

Cuadro 3.15: Valor agregado de Blockchain

	Anteriormente sin Blockchain	**Actualmente con Blockchain**	**Comparaciones**
Archivos e Información publicada de nivel de río	**1 solo archivo**	**Hash+Archivo+Comprobante**	**Mayor transparencia** con **Blockchain** ya que se publica el certificado y el hash en la página para validar
Registro	**Centralizado**	**Descentralizado**	**Mayor disponibilidad** con **blockchain** en caso de que un nodo de registro se vea afectado
Manipulación del nivel de Río	**Toneladas de carga perdida en buques y Mayores Costos U$S**	**0 cargas perdidas 0 costos perdidos**	**Mayor Integridad** con **blockchain** en caso de que se modifique algún dato publicado, la manipulación se detecta.

Fuente: Elaboración propia

Por lo tanto con Blockchain se tiene mayor confiabilidad en la información, garantía y seguridad (Figura 3.35). Es decir PNA con la cadena de bloques es una institución con divulgación de la información confiable a través de su página web.

Figura 3.35: Valor agregado de la información publicada de registros de altura de ríos

Fuente: Adaptado de presentación BFA Altura de Ríos

Figura 3.36: Resultados de aplicar *Blockchain*

Fuente: Adaptado de presentación BFA Altura de Ríos

La Organización marítima Internacional (*OMI*) introdujo el 16 de Junio de 2017 un nuevo concepto denominado Riesgo Cibernético Marítimo (Resolución MSC.428(98)), esto es una iniciativa para contribuir a la seguridad y protección del transporte marítimo, esto a través de directrices o recomendaciones para gestionar y afrontar los riesgos cibernéticos

marítimos. La PNA sigue esa línea de prevención ante vulnerabilidades y posibles ciberataques a la infraestructura de la información, las redes y los sistemas de comunicación. Por tal razón el uso de *blockchain* en los registros contribuyen a una mayor seguridad y protección del transporte marítimo.

Capítulo 4. Discusión

Se hizo un repaso desde el surgimiento de Internet y como ha revolucionado el acceso a la información, pasando a ser de una mensajería de correos a intercambiar todo tipo de datos hasta conformar una plataforma o ecosistema de interconexión en el mundo. Según el informe de la Unión Internacional de Telecomunicaciones en el año 2018 los usuarios de Internet superaba los 4000 millones, representando más de un 50% de la población mundial.

Pero el potencial es mayor aún y está en la base de la tecnología de las criptomonedas con el *Blockchain* y es por eso que se describieron los distintos casos de uso que van surgiendo en el mundo.

Actualmente un informe del Observatorio y Foro *Blockchain* de la Unión Europea muestra un mapa de iniciativas *Blockchain* de más de 700 casos de uso Financiero y no Financiero en todo el mundo:

Figura 4.1: Mapa mundial de iniciativas de *Blockchain*

Fuente: European *Blockchain Observatory* and *Forum* (2020)

También hay muchos *papers* desde el ámbito universitario, mostrando el interés de casos de usos con los *Smart Contracts.*

Dada todas las posibilidades de plataformas existentes de *Blokchain* junto a las distintas aplicaciones en distintos sectores tanto público, privado y las ONG, sirvió mucho haber clasificado los casos de usos tal como lo indica el Cuadro 2.2, permitiendo identificar claramente iniciativas de aplicación. También se identificaron empresas y países sumándose a la carrera de adoptar a futuro una tecnología innovadora. Los casos de usos muestran claramente que todavía la adopción de *Blockchain* está en desarrollo tal como indica el gráfico de *Gartner* Figura 2.5.

Uno podría hacer un resumen de casos de uso donde se identifique de forma más general y se clasifique en casos de uso como Registros, Trazabilidad y Contratos, tal como se muestra en el Cuadro 4.1.

Cuadro 4.1: Resumen de Casos de uso

Registros	Trazabilidad	Contratos
Registros médicos	Ingredientes alimenticios	Seguros
Registros de propiedad	Obras de arte	Seguridad automática
Registro de vehículos	Diamante	Alquiler
Registro de Propiedad Intelectual	Agricultura	Medios de comunicación
Servicios de notaría	Donaciones	Licencias de música
Sistema de Votación		Mercado de Electricidad
Identidad Digital de personas		
Identidad Digital de organizaciones		
Identidad Digital de dispositivos		
Internet de las cosas		
Internet		

Fuente: Elaboración propia

Se puede ver en el cuadro anterior, la mayor cantidad de ideas e iniciativas en Registros en *Blockchain*, luego le sigue la Trazabilidad es decir hacer un seguimiento de registros. Y por otro lado los casos de uso de Contratos, un acuerdo de dos o más partes plasmado a través de un *Smart Contract* desplegado en *Blockchain*.

De los casos de Registros se encuentra en relevancia el *Proof of Existence* (Prueba de Existencia) para registrar toda clase de documentos en *Blockchain*.

El hecho de usar en forma gratuita la plataforma BFA (Blockchain Federal Argentina) para certificaciones de archivos como el *Proof of Existence* es de ventaja a comparación de usar una plataforma pública como *Bitcoin*, el cual este tiene un costo para realizar transacciones y una dificultad alta de generar el bloque por el costo computacional y energético como se observa en el cuadro de comparación Cuadro 4.2.

En el siguiente Cuadro 4.2 se puede observar el resumen de los casos de usos de prueba de existencia con sus respectivas características:

Cuadro 4.2: *Proof of Existence* en distintas plataformas

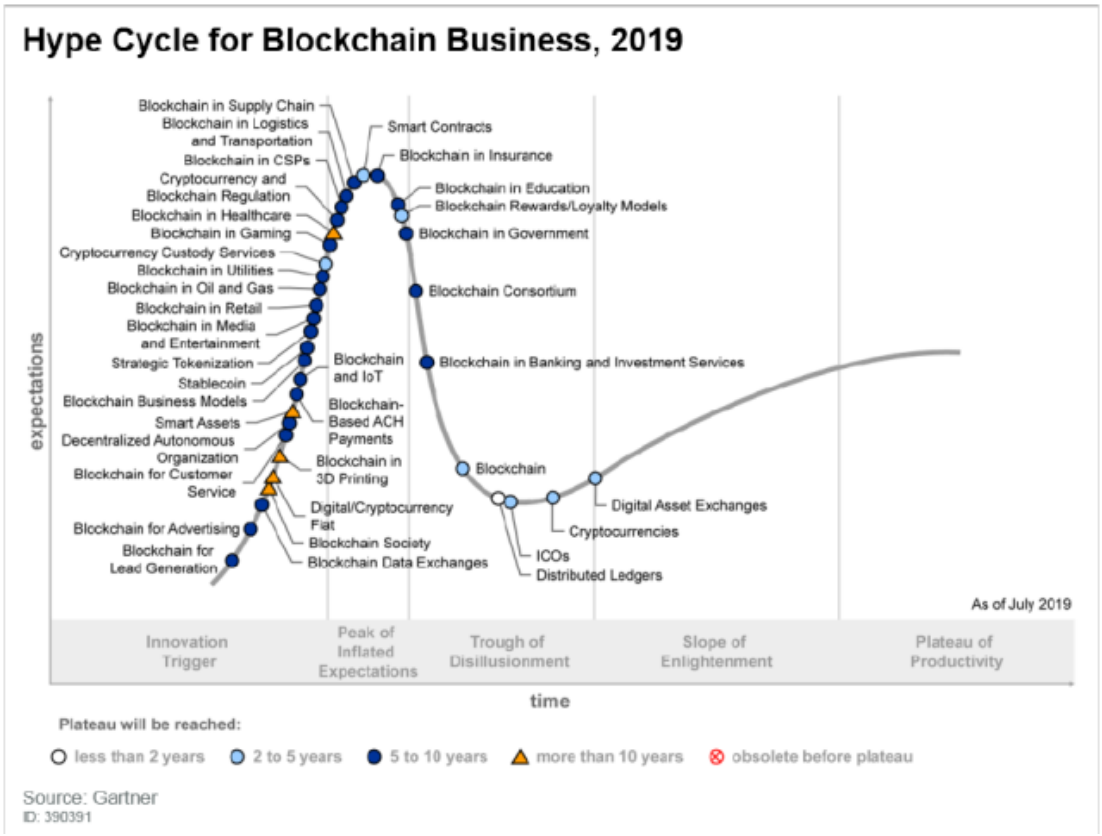
Casos de Uso	Tipo de Red	Tipo de Consenso	Dificultad de generar el bloque
Registros	Bitcoin	Prueba de Trabajo	Alta
Registros	Ethereum	Prueba de Trabajo	Media
Registros	Ethereum/BFA	Prueba de Autoridad	Baja

Fuente: Elaboración propia

El caso de uso de *Proof of Existence* es de interés dada la importancia de casos de uso del Cuadro 4.1 y son cada vez más los países sumándose en aplicaciones de registros en cadena de bloques. Y es por eso en este trabajo se demuestra como registrar un archivo con el caso de uso de Altura de Ríos siendo una iniciativa para comprobar realmente el funcionamiento de la plataforma multisectorial de Blockchain Federal Argentina.

Es claro, todavía queda un camino por recorrer para la maduración de la tecnología y se concientice de su uso. Pero son cada vez más los *stakeholders* sumándose a usar la cadena de bloques. Y en el caso del sector público otro gráfico de *Gartner* más actual como en la Figura 4.2 indica a *Blockchain* en Gobierno, se estima a adoptar esta tecnología de 5 a 10 años.

Figura 4.2: Gráfico de *Gartner* de Aplicaciones *Blockchain*



Fuente: Smart Gartner (2019)

Todavía queda por establecer un Centro de operaciones de Red en BFA y sirva de monitoreo y garantice la estabilidad de la plataforma. Y también el sumar más casos de usos para probar la escalabilidad de *Blockchain* con los contratos inteligentes, algo muy discutido en varios informes actuales sobre la cadena de bloques en el mundo.

El hecho de adoptar una tecnología innovadora en la organización pública implica a acordar con todos , sector público, privado, académico y sociedad civil, estableciéndose una especie de Gobernanza de Internet pero en este caso enfocado a *Blockchain*, donde haya políticas públicas que fomenten la adopción junto a regulaciones, creando así todo un ecosistema de actores debatiendo reglas claras de uso.

En el Anexo de este trabajo se agregan eventos y noticias de interés en relación a lo que es *Blockchain*, BFA y de su importancia a nivel nacional.

Dada la plataforma pública conformada de Blockchain Federal Argentina del tipo de consenso Prueba de Autoridad y en el cual en forma práctica la Prefectura Naval Argentina pudo ser parte como nodo sellador, se demuestra y se verifica que el nodo de PNA realmente es parte de la generación de bloques ajustándose a la tecnología y a uno de los tipos de consenso mencionado en el marco teórico.

Se toma el caso de uso de *Proof of existence* plasmado en un *Smart Contract* de la institución y desplegado en la red BFA y de allí poder interactuar mediante la interfaz de la aplicación para el registro de certificados de Altura de Ríos.

Las dificultades fueron una mezcla de todo, desde que PNA es parte de ser nodo sellador y empezar a entender en que consistía la Blockchain y superado esta dificultad luego vino la dificultad de como desplegar el primer Smart Contract en la institución. Luego surgieron otras dificultades de tener un entorno de desarrollo porque uno en *google* o en *youtube* (y con ayuda de reuniones técnicas de orientación) se puede encontrar con ejemplos de distintas formas de entornos de desarrollo.

En fin se eligió el entorno para desplegar Smart Contracts con *Visual Studio Code* junto a las herramientas de *Truffle.*

Y así dando lugar a la primera aplicación de Prefectura Naval Argentina como una de las primeras autoridades marítimas en hacer uso de *Blockchain.*

Riesgos

Otros aspectos a tomar en cuenta es la seguridad en la tecnología *Blockchain* debido a las amenazas posibles como : la Ingeniería social para la obtención de direcciones de cuentas a través de las redes sociales, el uso de *Blockchain* como servicio en la nube, el descuido de uso de dispositivos conectados a la red *Blockchain* en cuanto a la no protección y posibilidad de virus y también la amenaza de propias personas pertenecientes a la organización con *Blockchain.*

La seguridad brindada por *Blockchain* es la confidencialidad complementaria con la autenticación del usuario para el acceso a las transacciones, también está la integridad de que la información de los bloques no se modifique ni se pierda y esto acompañado con necesidad de contar con un mayor números de nodos de red para evitar un ataque conocido como el 51% de capacidad computacional de los nodos. Es decir si se lograra tener el 51 % de la capacidad de la red de nodos se puede generar que se rompa la cadena, generando otros bloques permitiendo por ejemplo el doble gasto. Por último la tecnología de *Blockhain* asegura el conocimiento de quien envía y recibe en las transacciones.

Los ataques que pudiera sufrir la cadena es tener el control de la red a través de la capacidad del 51 % , como ya se mencionó anteriormente, esto es algo de importancia en las *Blockchain* públicas en cambio en las *Blockchain* privada se evita teniendo mejor el conocimiento a quienes se dan acceso a la red de nodos. Otro ataque que se ha producido en la práctica es la maleabilidad de las transacciones es decir parte de esta es modificable a tal punto de modificar su *hash* correspondiente, esto se ha solventado actualmente en *Bitcoin*. También el uso de la *Blockchain* pública *Ethereum* lo ha solucionado.

El uso de la Blockchain Federal Argentina (BFA) es una *Blockchain* federada donde los nodos generadores de bloques son autorizados y reconocidos dentro de la red, con esto se evita el riesgo de que algún anónimo este haciendo uso de la red para intentar modificar algún registro en la cadena de bloques.

También en BFA se hace uso de nodos denominados gateway y con esto se evita a usuarios o miembros estén generando abuso del uso de transacciones en la red.

El almacenamiento en BFA es solo de hash, la plataforma no funciona como nube para almacenar archivos.

Capítulo 5. Conclusiones y propuestas

Por lo tanto se pudo comprobar la hipótesis planteada al inicio, se ve la importancia de *Blockchain* más allá de las criptomonedas como son los casos de usos no financieros. Y de relevancia se vió en este trabajo el potencial de uso de *blockchain* en registros públicos y privados mencionados en *papers*, páginas *webs* informativas, Gráfico de *Gartner*, especialistas y estudios de iniciativas en muchos países del mundo. Y en particular respecto al registro de algún documento en la cadena de bloques en el sector público como es el caso de aplicación con el *Proof of Existence*.

Es de interés el uso de *Blockchain* para el sector público porque brinda valor agregado a los procesos de registros respecto en la descentralización de la información, integridad, seguridad y velocidad de registro.

Sumando también la experiencia de ser parte y participar del proyecto Blockchain Federal Argentina realizando la iniciativa del caso de uso para Prefectura Naval Argentina.

La tecnología *Blockchain* da validez de confianza y la plataforma conformada BFA es de utilidad para un Organismo Público para hacer uso de registros de documentos como es el caso de Altura de Ríos brindando seguridad, confiabilidad y transparencia de la información que se publica.

El hecho de poder haber experimentado un entorno de desarrollo con esta nueva tecnología con una aplicación, se verifica en forma práctica el funcionamiento de *Blockchain* dentro de una organización, siendo así parte de una Transformación Digital de cómo llevar a cabo los procesos de registro de documentos.

La plataforma a la cual es parte la Prefectura Naval Argentina brinda la posibilidad a múltiples aplicaciones a futuro entre ellas la de interés como trazabilidad.

Como desafío a futuro es poder usar un caso de uso de trazabilidad y creo que es el interés de muchos *stakeholders*, otro desafío es poder tener otros entornos de desarrollo e

incentivar dentro y fuera de la institución el uso de *Blockchain* aumentando los casos de uso y el equipo de trabajo.

También se innova en la forma de trabajar para realizar el proyecto de *Blockchain* nacional siendo colaborativo y participativo, hoy en día innovación no es el trabajo de una sola persona sino que es una cultura constructiva donde se genera una base de sinergias con la colaboración de todos y es eso lo que se llevó a cabo en la BFA.

Bibliografía

Alharby,M.; Aldweesh,A. y Moorsel, A.(2018).Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research. Paper. School of Computing, Newcastle University. Newcastle upon Tyne, UK.

AV-TEST(2020). Cifras y análisis de la actual situación de riesgo: Informe de seguridad 2019/2020.[En línea]. Disponible en: https://www.av-test.org/es/noticias/cifras-y-analisis-de-la-actual-situacion-de-riesgo-informe-de-seguridad-2019-2020-de-av-test/

BFA (2019). Evento Blockchain Federal Argentina : Exposición de iniciativas de aplicaciones. [En línea]. Disponible en: https://bfa.ar/bfa19

Bit2Me Academy (2020). Smart Contracts: ¿Qué son , cómo funcionan y qué aportan?. [En línea]. Disponible en: https://academy.bit2me.com/que-son-los-smart-contracts/

Bit2Me Academy (2020). Qué es Prueba de trabajo. [En línea]. Disponible en: https://academy.bit2me.com/que-es-proof-of-work-pow/

Blockchain Economía (2019). Se lanza la primera blockchain mundial para ONGs y Fundaciones desde España. [En línea]. Disponible en: https://www.blockchaineconomia.es/blockchain-mundial-para-ongs/

Blog Universidad Politécnica de Valencia (2011).Historia de las Bases de Datos.[En línea]. Disponible en: https://histinf.blogs.upv.es/2011/01/04/historia-de-las-bases-de-datos/

Bolsa de Comercio de Rosario (2018). La bajante del Paraná y su impacto en el complejo oleaginoso del Gran Rosario. (Documento Informativo Semanal)

Bolsa de Comercio de Rosario (2018). La notable infraestructura portuaria en el tramo Puerto Cáceres (Brasil)- Gran Rosario. (Documento Informativo Semanal)

Bolsa de Comercio de Rosario (2020). Río Paraná: la bajante más severa en los últimos 50

años representa un costo de US$ 244 millones para el complejo agroexportador. (Documento Informativo Semanal)

Buterin, V.(2014). A next-generation smart contract and decentralized application platform.White Paper.

CABASE (2020). Cámara Argentina de Internet. [En línea]. Disponible en: https://www.cabase.org.ar/la-camara/

Chambi Villarroel, G.D.(2019). Certificado de Altura de Ríos. [En línea]. Disponible en: https://bfa.ar/bfa/presentaciones

Consensys (2020). The State of the Ethereum Network: 5 Years Running. [En línea]. Disponible en: https://consensys.net/blog/news/the-state-of-the-ethereum-network-2020/

Criptonoticias (2015). Blockchain: bloques,transacciones,firmas digitales y hashes.[En Línea]. Disponible en : https://www.criptonoticias.com/criptopedia/blockchain-bloques-transacciones-firmas-digitales-hashes/

Deloitte (2017). Will blockchain transform the public sector?. UK: Deloitte University Press. (Artículo)

Dolader, Bel y Muñoz (2017). La Blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. Paper. Universitat Politécnica de Catalunya.

Durán, M. M.(2012). El estudio de caso en la investigación cualitativa. Revista Nacional de Administración, Volumen 3, Número 1, 2012, pp. 121-134. Escuela de Ciencias de la Administración,Universidad Estatal a Distancia. Costa Rica. [En línea]. Disponible en: https://revistas.uned.ac.cr/index.php/rna/article/view/477/372

El País Financiero (2020). Bitcoin: Qué es, como funciona y por qué ha llegado para quedarse.[En línea]. Disponible en: https://elpaisfinanciero.com/bitcoin/

El Economista (2017). Ethereum es Turing completo ¿y eso qué es?. [En línea]. Disponible en: https://www.eleconomista.es/economia/noticias/8817210/12/17/Ethereum-es-Turing-completo-y-eso-que-es.html

Ethereum (2016). Introducción a los Contratos Inteligentes. [En línea]. Disponible en: https://solidity-es.readthedocs.io/es/latest/introduction-to-smart-contracts.html

Ethereum community (2016). What is Ethereum?. [En línea]. Disponible en: https://ethdocs.org/en/latest/introduction/what-is-ethereum.html#a-next-generation-blockchain

EUBlockchain (2020) .Observatory and Forum : Initiative Map in the world. Disponible en: https://www.eublockchainforum.eu/initiative-map

Evento BFA (2019). Blockchain Federal Argentina. [En línea]. Disponible en: https://www.youtube.com/watch?v=qBTCRDl-Dg0

FortiGuard Labs (2021). Threat Map. [En línea]. Disponible en: https://www.fortiguard.com/threat-research/map

Fortinet (2020). Fortinet Threat Intelligence Insider Latin America. (Boletín Informativo)

Gartner (2017). Hype Cycle for Emerging Technologies. [En línea]. Disponible en: http://www.bigdata-social.com/hype-cycle-digital-workplace-2017-gartner/

Gitlab BFA (2019). Repositorio de Blockchain Federal Argentina. [En línea]. Disponible en: https://gitlab.bfa.ar/blockchain

IBM (2017). The difference between public and private blockchain. [En línea]. Disponible en: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

INTERPOL (2020). Ciberdelincuencia: Efectos de la COVID-19. (Reporte)

Misiones Online (2020). El Paraná en su bajante histórica complica la logística para barcazas que transportan granos. [En línea]. Disponible en: https://misionesonline.net/2020/04/09/el-parana-en-su-bajante-historica-complica-la-logistica-para-barcazas-que-transportan-granos/

Mukhopadhyay, M. (2018). Ethereum Smart Contract Development. Inglaterra: Packt Publishing. (Libro)

Nakamoto, S.(2008). Bitcoin : A peer-to-peer electronic cash system.[En línea]. Disponible en: https://bitcoin.org/bitcoin.pdf

Néstor Altuve (2019). Explorando el potencial de la tecnología Blockchain en la organización. [En línea]. Disponible en : https://nestoraltuve.com/2019/08/08/explorando-el-potencial-de-la-tecnologia-blockchain-en-la-organizacion/

NIC Argentina (2017). 30 años de NIC Argentina (.ar) en el marco de la evolución de Internet.[En línea]. Disponible en: https://nic.ar/es/enterate/novedades/30-anos-de-nic

Observatorio FinTech (2016). 15 aplicaciones de la tecnología blockchain más allá de bitcoin.[En línea]. Disponible en: https://www.fin-tech.es/2016/10/aplicaciones-de-la-tecnologia-blockchain.html

Prefectura Naval Argentina (2021). OMI: Recomendación para la gestión de los riesgos cibernéticos marítimos. Disponible en: https://www.argentina.gob.ar/prefecturanaval/seguridadnavegacion/buques/recomendacion-riesgos-ciberneticos-maritimos

PEM(2004). Plan estratégico metropolitano Región Rosario. .[En línea]. Disponible en: http://biblioteca.municipios.unq.edu.ar/modules/mislibros/archivos/DocumentoBaseFinal.pdf

Preukschat, A. (2017). Blockchain: la revolución industrial de internet. España: Gestión 2000. (Libro)

Proof of Existence (2020). What is Proof of Existence?. [En línea]. Disponible en: http://docs.proofofexistence.com/#/?id=what-is-proof-of-existence

Ranjeet Patel (2020). Byzantine Fault Tolerance (BFT) and its significance in Blockchain world. [En línea]. Disponible en: https://www.hcltech.com/blogs/byzantine-fault-tolerance-bft-and-its-significance-blockchain-world

Retina (2018). ¿A qué se destina el dinero de una ONG? Con blockchain podrás saberlo. [En línea]. Disponible en: https://retina.elpais.com/retina/2018/04/06/innovacion/1523027028_521263.html

Rocha, M. (2019). Fundamentos de Internet. Documento de Gestión de Redes, Módulo 1. LACNIC.

Rodriguez, N. (2018). La Mejor Guía sobre la Tecnología Blockchain: Una Revolución para Cambiar el Mundo.[En línea]. Disponible en: https://101blockchains.com/es/tecnologia-blockchain/

Rosario es más (2015). El Puerto de Rosario apuesta a la expansión. [En línea]. Disponible en: https://www.rosarioesmas.com/page/noticias/id/39/title/El-Puerto-de-Rosario-apuesta-a-la-expansión

Anexos

Stakeholders

Se puede citar muchas opiniones y noticias de hoy en día, involucrando a todo tipo de organismos y personas.

Cada vez es más la opinión y el interés de los distintos *stakeholders* de los beneficios de *Blockchain*, no solamente en moneda virtual o criptomonedas sino en distintas áreas de aplicación y en la misma sociedad, es un cambio de paradigma con esta nueva tecnología.

He asistido a muchas reuniones técnicas de Blockchain Federal Argentina donde se trataban y se sigue tratando el interés de ir armando la infraestructura con el aporte de cada parte que va conformando la plataforma Blockchain. Los que participan en las reuniones técnicas proponen avances de aplicaciones, monitoreo, pruebas de stress de la red, presentaciones y eventos a definir. El material en documentos de avances puede encontrarse en el repositorio de *Gitlab* BFA.

A continuación los artículos y eventos.

Artículo de Infobae 28 de Julio de 2018:

Argentina lanza una plataforma en blockchain para mejorar los procesos públicos

Publicación de Infobae, mencionando a Blockchain Federal Argentina en su inicio de plataforma y los beneficios de la tecnología para distintos sectores de la sociedad. Con la importancia que tendrá la plataforma de valerse de una bitácora de transacciones públicas, segura e inmutable. Será una plataforma multiservicios que permitirá la utilización de aplicaciones pensadas para la realización de contratos, transacciones y otras operaciones en un entorno asegurando transparencia , eficiencia y seguridad.

https://www.infobae.com/cripto247/mercados/2018/07/28/argentina-lanza-una-plataforma-en-blockchain-para-mejorar-los-procesos-publicos/

Artículo de Ámbito Financiero 20 de Marzo de 2019:

Blockchain: dos casos de empresas argentinas

Nicolás Mayer-Wolf CEO de la empresa Agree Market habla de la importancia de uso de Blockchain, hoy la empresa cuenta con una plataforma online para hacer más eficiente la comercialización de commodities agrícolas. Con la cadena de bloques hay un cambio radical en la industria, principalmente en lo que se refiere a seguridad, trazabilidad y transparencia. Dentro de esta plataforma se permite asegurar la inmutabilidad de las negociaciones y los contratos que se celebran, es una manera de certificar que lo transaccionado no fue manipulado o modificado. Pablo Pereira CEO de la empresa Everis Argentina, también habla de la importancia de Blockchain en numerosas situaciones de negocio en las cuales es necesario autenticar algo. Everis fue un precursor en el desarrollo de soluciones basadas en blockchain y activo involucramiento en la formación y desarrollo de la red Alastria en España Siendo Alastria un consorcio con activa participación de las principales compañías españolas que identifica y desarrolla casos de uso basados en blockchain.

Everis en la región está activamente trabajando en conjunto con el banco Interamericano de Desarrollo en la puesta en marcha de LaCChain que tiene objetivos parecidos a Alastria.

Además, Everis es la primera compañía privada que tiene nodos en BFA (Blockchain Federal Argentina).

https://www.ambito.com/negocios/blockchain/dos-casos-empresas-argentinas-n5021712

Artículo de Criptonoticias 22 de Octubre de 2019:

Blockchain Federal Argentina presenta sus nuevos miembros y avances de casos de uso

El periódico digital Criptonoticias informa del evento llevado a cabo el 22 de Octubre de 2019 en la Facultad de Ingeniería de la Universidad de Buenos Aires. En este evento distintas entidades públicas y privadas expusieron las iniciativas de casos de uso en la plataforma Blockchain Federal Argentina. El artículo habla del funcionamiento de la plataforma argentina donde se opta por el modelo de consenso de Prueba de Autoridad y no se tiene costo por usar esta red blockchain.

https://www.criptonoticias.com/comunidad/adopcion/blockchain-federal-argentina-nuevos-miembros-casos-uso/

Gudnar Chambi Villarroel:

Conferencia en la Universidad Gabriel René Moreno en Santa Cruz de la Sierra – Bolivia

Estuve como expositor en la Conferencia de Blockchain en la Universidad Autónoma Gabriel René Moreno, Santa Cruz de la Sierra, Bolivia, el día 8 de Febrero de 2019.

Explicando el concepto de la tecnología blockchain y su funcionamiento.

Estuvieron presentes el Msc. Ing. Saul Severiche, Director de la carrera Electrónica de la Universidad Gabriel René Moreno y otras autoridades junto a alumnos, interesados en el conocimiento de la tecnología de la cadena de bloques.

Evento BFA Facultad de Ingeniería Universidad de Buenos Aires

También presenté el caso de uso de Blockchain de Altura de Ríos de Prefectura Naval Argentina en la Facultad de Ingeniería Universidad de Buenos Aires, el día 21 de Octubre de 2019 Evento BFA. La presentación de este evento se puede encontrar en la página bfa presentaciones.

BFA '19

CERTIFICADOS DE ALTURA DE RÍOS

Gudnar Chambi Villarroel
Ingeniero de Redes en la Dirección de Informática y Comunicaciones de Prefectura Naval Argentina

Glosario

ARIU: Asociación de Redes de Interconexión Universitaria.

BFA: Blockchain Federal Argentina.

BGP: Protocolo de ruteo en redes.

CABASE: Cámara Argentina de Internet.

Carriers: Empresas que brindan infraestructura de Internet con rutas de conexiones regionales.

Core: Parte central de una red de telecomunicaciones que provee varios servicios a usuarios que se conectan a través de la red de acceso.

DNS: Domain Name System (sistema de nombre de dominio) es un servicio para resolver nombres de páginas de internet.

ECDSA: Elliptic Curve Digital Signature Algorithm (Algoritmo de firma digital de curva elíptica). Este algoritmo es usado en Bitcoin y Ethereum para generar claves públicas a partir de claves privadas. También ese usado para firmar o verificar las transacciones.

Ether: La moneda para transacciones utilizada en la blockchain ethereum.

Fintech: Industria financiera que aplica nuevas tecnologías a actividades financieras y de inversión.

Hash: es una función criptográfica especial utilizada para la generación de identificadores únicos e irrepetibles.

Hascash: Algoritmo usado en el protocolo de consenso de trabajo en bitcoin.

Insurtech: empresas de tecnología centradas en la industria del seguro.

IXP: Punto de Interconexión de Internet.

LACNIC: Es el Registro de Direcciones de Internet de América Latina y Caribe, una organización no gubernamental internacional.
Minero

NICar: Centro de Información de la Red para Argentina, una oficina dependiente de la Secretaría Legal y Técnica de la Presidencia de la Nación. NIC Argentina administra el Registro de nombres de dominio y asegura el funcionamiento del DNS.

Nodo sellador: Nodo de la red blockchain cuya función es agregar bloques.

Nodo transaccional: Nodo de la red blockchain cuya función es enviar transacciones para su agregado en la cadena de bloques por nodos selladores.

Nonce: Número secuencial usado para la generación de hash en la búsqueda de hash en un protocolo de prueba de trabajo.

Número de Sistema Autónomo: Identificador para establecer la conexión de ruteo BGP.

ONG: Organización No Gubernamental, son organizaciones que no son parte de las esferas gubernamentales o empresas cuyo fin fundamental es el bien social.

PNA: Prefectura Naval Argentina.

Proof of work: En español significa Prueba de Trabajo, es un protocolo de consenso conocido con Bitcoin, usado para generar un bloque mediante el uso de resolución de un problema matematico en la tecnología de blockchain.

Proof of Authority: En español significa Prueba de Auotridad, es un protocolo de consenso donde los bloques de la cadena sólo pueden ser agregados por nodos autorizados.

Peer to peer: red de pares.

Proof of Stake: En español significa Prueba de Participación, es un protocolo de consenso donde los bloques de la cadena solo pueden ser agregados por nodos con mayor cantidad de tokens o tengan mayor participación en la red.

SHA-256: Algoritmo o función criptográfica para generar una cadena fija de caracteres.

Número de Sistema Autónomo: Identificador para establecer la conexión de ruteo BGP.

Script: es un lenguaje de programación que ejecuta diversas funciones en el interior de un programa de computador.

Smart Contracts: Contratos inteligentes donde se establece a través de códigos una programación o acuerdo entre partes en blockchain.

Stakeholders: Partes interesados.

TCP: Transmission Control Protocol.Protocolo de Internet.

Token: Los tokens son representaciones de valor basados en Blockchain.

Turing Complete: Turing completo, sistema en el que se pueda programar para cualquier tipo de operación.