Universidad de San Andrés

Escuela de Negocios

Maestría en Gestión de Servicios Tecnológicos y de Telecomunicaciones

Implementación de folio real digital en el Registro Nacional de Buques con tecnología blockchain

Autor: Ing. Ernesto Miguel Klocker

DNI: 14.742.060

Director de Tesis: Ing. Enrique Hofman

Buenos Aires, Mayo de 2020

Universidad de San Andrés

Escuela de Administración y Negocios

Maestría en Gestión de Servicios Tecnológicos y de Telecomunicaciones

Implementación de folio real digital en el Registro Nacional de Buques con tecnología blockchain

Autor: **Ing. Ernesto Miguel Klocker**

DNI: **14.742.060**

Director de Tesis: **Ing. Enrique Hofman**

Maestría: **Gestión de Servicios Tecnológicos y de Telecomunicaciones**

Director Académico: **Ing. Enrique Hofman**

Buenos Aires, Mayo de 2020

Contenido

QUAERERE VERUM
Universidad de
SanAndrés

Introducción

Blockchain ha venido a constituirse en uno de los pilares de la transformación digital, y muchos analistas coinciden en que traerá aparejado importantes cambios en el modo en que nos relacionamos en muchos aspectos de nuestra vida cotidiana. Esta tecnología emergente promete modificar algunos modelos de negocios y su potencial abre las puertas a nuevos modos de interacción, al punto que hay quienes sostienen que podría revolucionar por completo internet.

La tecnología blockchain posibilita realizar transacciones de manera segura, confiables e irreversibles, eliminando la necesidad de un intermediario de confianza. Sus transacciones son imposibles de falsificar o borrar una vez registradas. Estas transacciones si bien son públicas, las partes permanecen anónimas y la base de datos contiene un histórico de todas y cada una de las operaciones.

Las características de inmutabilidad, trazabilidad, seguridad, robustez, consenso distribuido y transparencia hacen de blockchain un modelo de transparencia abierto y participativo, pero a la vez seguro, que se orienta a la eficiencia en los procesos y la definición de nuevos modelos de negocio que resuelvan necesidades de los consumidores y de la sociedad.

Blockchain es todavía una tecnología incipiente y en pleno desarrollo, con desafíos tecnológicos y legales aún por resolver; por ello resulta interesante desarrollar caso de uso para aplicaciones concretas y así poder evaluar su rendimiento.

En este trabajo, se abordará como caso de uso la implementación del Folio Real en el Registro Nacional de Buques argentino, usando tecnología blockchain para garantizar la trazabilidad e inmutabilidad de las anotaciones, tendiendo a evaluar y validar su aplicación para extender su uso en otros casos de la administración pública.

Abstract

Blockchain has become one of the pillars of digital transformation, and many analysts agree that it will bring about important changes in the way we interact in many aspects of our daily life. This emerging technology promises to modify some business models and its potential opens doors to new modes of interaction, to the point that there are those who argue that it could completely revolutionize the internet.

Blockchain technology enables transactions to be made safely, reliably and irreversibly, eliminating the need for a trusted intermediary. Its transactions are impossible to falsify or delete once registered. Although these transactions are public, the parts remain anonymous and the database contains a historic file of each and every one of the operations.

The characteristics of immutability, traceability, security, robustness, distributed consensus and transparency make blockchain an open and participatory model of transparency, but at the same time secure, which is oriented to the efficiency in the processes and the definition of new business models that solve the needs of consumers and society.

Blockchain is still an incipient and developing technology, with technological and legal challenges still to be solved; therefore, it is interesting to develop a use case for specific applications and thus be able to evaluate its performance.

In this work, the implementation of the Real Folio in the Argentine National Ship Registry will be addressed as a use case, using blockchain technology to guarantee the traceability and immutability of the annotations, tending to evaluate and validate its application to extend its use in other cases of the public administration.

Capítulo 1 - Descripción del Proyecto

Justificación del proyecto

Descripción del problema que se intenta resolver

En los últimos años en la República Argentina se han incorporado nuevas normativas y actualizado las existentes en el marco del proceso de modernización de la Administración Pública Nacional, tendientes a la optimización de la infraestructura tecnológica de los distintos organismos del Estado, fortalecimiento de la infraestructura tecnológica de firma digital, como así también se ha avanzado en la identificación de tecnologías de la información innovadoras y emergentes a nivel mundial y regional, para evaluar la viabilidad de su posible adopción.

En este marco, y estando en curso el proceso de implementación de un sistema de gestión integral en el Registro Nacional de Buques -encargado de la matriculación y el registro de embarcaciones nacionales- y su inter-operatividad con el sistema de Gestión Documental Electrónica (GDE) y Trámites a Distancia (TAD), surge la necesidad de mejorar y optimizar las características de seguridad e inmutabilidad del Folio Real, documento registral donde se plasma la situación dominial de los buques.

El Folio Real del tipo “cartular”, requiere que los asientos se efectúen en un formulario con soporte papel (cartón), acompañando con la firma ológrafa de escribano o funcionario del registro interviniente para su validación. Estos asientos son posteriormente - en forma asincrónica - cargados en un sistema informático y quedarán disponibles para el propio Registro u otras áreas u organismos de la administración.

Al momento de dar certidumbre sobre la información registral, los escribanos se sólo dan fe sobre los datos volcados y rubricados en el folio real cartular (FRC) tenido a la vista; evitando pronunciarse en relación a los datos cargados en las base de datos de los sistemas de información, ya que pueden variar respecto de los asientos registrados en el cartón, por el diferimiento de tiempo que existe en la carga de datos al sistema, posibles errores en el volcado de datos o cualquier otra transformación en los datos producto de una acción culposa o dolosa por podría ocurrir parte del operador del sistema.

La implementación de un Folio Real electrónico-cartular (FREC), es decir generado electrónicamente a partir de datos previamente cargados en el sistema, pero luego impreso y firmado en el soporte cartular, fue considerada inicialmente como una opción válida por parte del Registro; pero a poco de ser puesta en práctica fue descartada al corroborarse que no resolvía el problema de la inconsistencia de la información entre el soporte físico y el digital, al detectarse trámites que fueron resueltos incorporando asientos con máquina de escribir en folios cartulares, sin el correspondiente correlato en el sistema y la base de datos.

Con un Folio Real Digital (FRD), generado electrónicamente desde el sistema de gestión y firmado digitalmente, se logran resolver los problemas apuntados. Cada vez que se produce un nuevo asiento, se genera una nueva “versión” del folio real digital. La situación registral de un buque, será entonces la que en definitiva exponga el último folio real digital vigente que existe en la base de datos. Este folio real, firmado digitalmente por el escribano interviniente, refleja todas las intervenciones de escribanos anteriores. En este estado, se torna imprescindible garantizar que no se haya omitido o alterado el

contenido del folio real; ya que la situación registral del buque, será la que surge de la última versión del folio real digital válida.

La preservación de la serie histórica de folios, queda en cabeza del administrador o responsable de la base de datos y del repositorio de documentos digitales; funcionario que no necesariamente perteneciente al propio Registro y que tiene que poder garantizar y demostrar -mediante sus propios logs y registros- la integridad e inalterabilidad de las transacciones contenidas en la base de datos. Dicho de otro modo, tiene que poder dar acabadas pruebas de la existencia de cada versión del folio real digital y que no se ha omitido ninguna. Por su parte el Registro, no posee de ninguna herramienta práctica y efectiva para chequear la inalterabilidad del folio.

Lograr que manera indubitable que el Registro Nacional de Buques tenga fehacientes pruebas del estado de los folios reales digitales, sin tener que depender de los registros del administrador del sistema, hará una gestión más transparente y confiable para todas las partes.

Preguntas de investigación

¿Es la tecnología blockchain apropiada para garantizar la prueba de existencia de un folio real digital en el registro nacional de buques?

¿Qué ventajas permitiría la tecnología blockchain en este proceso?

¿Qué tecnología blockchain es la más apropiada?

Hipótesis

La tecnología blockchain es apropiada para garantizar la integridad y conservación de los folios reales digitales del Registro Nacional de Buques y permite reemplazar adecuadamente los actuales folios cartulares y/o electrónicos existentes con adecuadas medidas de seguridad.

Objetivos

Se determinará si la tecnología blockchain es apropiada y aplicable para garantizar la prueba de existencia de los folios reales en el registro nacional de buques y permiten reemplazar adecuadamente los actuales folios cartulares y/o electrónicos existentes con adecuadas medidas de seguridad.

De no resultar aplicable, se precisará que dimensiones o factores individuales que impiden su utilización o aplicación para el caso de los folios reales.

En caso de introducirse la tecnología blockchain, se evaluará en qué grado mejora los procesos administrativos y la satisfacción del usuario interno y externo.

Se establecerán las medidas de seguridad y procesos que se deberán observar para garantizar la adecuada utilización de la tecnología.

Adicionalmente se tratará de establecer si el método o enfoque adoptado puede generalizarse en casos similares.

Alcance y limitaciones

El alcance del presente trabajo se limita a determinar si la tecnología blockchain resulta apropiada y conveniente para garantizar la prueba de existencia de los folios reales en el registro nacional de buques y permiten reemplazar adecuadamente los actuales folios cartulares y/o electrónicos existentes con adecuadas medidas de seguridad; desarrollando un caso de uso completo, para su implementación.

QUAERERE VERUM
Universidad de
SanAndrés

Capítulo 2 - Marco teórico

Metodología

Conforme la Resolución N° 160 del Ministerio de Educación de la Nación (MinEduc, 2011) la Maestría tiene por objeto proporcionar una formación académica y/o profesional, con el objeto de profundizar el conocimiento teórico, metodológico, tecnológico, de gestión, o artístico, en función del estado de desarrollo correspondiente a la disciplina, área interdisciplinaria o campo profesional de una o más profesiones, para cuyo egreso requiere de la presentación de un trabajo final individual escrito consistente en un proyecto, estudio de casos, obra, producción artística o tesis, según el tipo de Maestría, con especificación precisa de una sola de estas posibilidades: una disciplina, un área interdisciplinar, una profesión o un campo de aplicación.

En este sentido; existen dos tipos metodológicos de maestrías:

1) **Académica**, vinculada específicamente con la investigación en un campo del saber disciplinar o interdisciplinar; en que a lo largo de su desarrollo se profundiza tanto en temáticas afines al campo como en la metodología de la investigación y la producción de conocimiento en general y en dicho campo. El trabajo final de este tipo de maestría académica es una tesis que da cuenta del estado del arte en la temática elegida y de la implementación de una metodología de investigación pertinente a la misma.

2) **Profesional**, vinculada específicamente con el fortalecimiento y consolidación de competencias propias de una profesión o un campo de aplicación profesional; en el que se profundizan competencias en vinculación con marcos teóricos disciplinares o multidisciplinares que amplían y cualifican las capacidades de desempeño en un campo de acción profesional o de varias profesiones. En este caso, el trabajo final es un proyecto, un estudio de casos, una obra, una tesis, una producción artística o trabajos similares que dan cuenta de una aplicación innovadora o producción personal que, sostenida en marcos teóricos, evidencian resolución de problemáticas complejas, propuestas de mejora, desarrollo analítico de casos reales, muestras artísticas originales o similares y que estén acompañadas de un informe escrito que sistematiza el avance realizado a lo largo del trabajo.

El presente trabajo final de maestría se inscribe entonces en el **modelo de maestría profesional**, es decir adopta un formato de tesis, pero enfocada al desarrollo de un proyecto que permita evidenciar la integración de aprendizajes realizados en el proceso formativo, la profundización de conocimientos en el campo profesional específico y el manejo de destrezas y perspectivas innovadoras en la profesión.

Paradigmas de la investigación

Según Guba y Lincoln (Guba & Lincoln, 2002) existen cuatro paradigmas que sustentan los diversos procesos investigativos: positivismo, post-positivismo, teoría crítica y constructivismo, y para que un investigador se posicione en uno de ellos debe responder a tres interrogantes: la pregunta ontológica ¿Cuál es la forma y naturaleza de la realidad?; la pregunta epistemológica ¿Cuál es la naturaleza de la relación entre el conocedor o el posible conocedor y qué es aquello que puede ser conocido? y la pregunta metodológica ¿Cómo el investigador puede descubrir aquello que él cree puede ser conocido?.

Dentro de tal contextualización, conciben que se buscara responder las preguntas mencionadas desde la perspectiva de cada uno de los paradigmas y finalmente, en base a las respuestas se determinará el método que más se ajusta al fenómeno de investigación.

En cada uno de los paradigmas, se ha respondido a los cuestionamientos ontológico, epistemológico y metodológico:

- **El positivismo** afirma que la realidad es absoluta y medible, la relación entre investigador y el fenómeno de estudio debe ser controlada, puesto que no debe influir en la realización del estudio. Los métodos estadísticos inferenciales y descriptivos son la base de este paradigma.
- **El post-positivismo** indica que la realidad es aprehensible de forma imperfecta por la propia naturaleza del ser humano. Los hallazgos son considerados como probables. En la metodología se pueden utilizar tanto métodos cuantitativos como cualitativos, sin embargo, estos últimos con un tinte hacia el positivismo más que al constructivismo, como lo desearían los partidarios clásicos del enfoque cualitativo.
- **La teoría crítica** considera a lo real como producto de un historicismo social. La relación entre el investigador y el objeto de estudio es importante, puesto que en su interacción se modifican las estructuras. La metodología clásica de este paradigma es la investigación-acción.
- **En el constructivismo** la realidad se construye mediante el interaccionismo simbólico de los sujetos que conforman un grupo social. La relación entre el investigador y el objeto de estudio permite construir la teoría sustantiva resultante en la investigación. El método clásico en este paradigma es la teoría fundamentada emergente.

El propósito de la presente investigación se inscribe dentro del paradigma de la teoría crítica, ya que pretende la transformación de las estructuras y se involucra, en la confrontación e incluso en el conflicto. El criterio de progreso, la dedicación y el activismo son conceptos claves. Se propone al investigador como un sujeto con en el rol de observador, instigador y facilitador del cambio; esto implica que el investigador presume a priori qué transformaciones cabrían aplicar y que necesita validarlas mediante el método científico. Debe apreciar las instancias más radicales en el campo crítico y que determinar los juicios sobre las transformaciones que propone introducir.

Enfoque de investigación

En el presente documento se realiza una investigación preliminar de la literatura disponible respecto las diferentes teorías y modelos desarrollados para evaluar, desde la perspectiva de la experiencia del usuario, el éxito en la adopción de la tecnología blockchain en diferentes países y en la industria; teniendo como objeto conocer las principales corrientes de investigación y los autores más destacados. El resultado de este ejercicio, sirve para orientar una investigación más profunda al momento de realizar la preparación de la tesis de maestría.

Recursos utilizados en la investigación

Para llevar adelante el presente trabajo de investigación, se accedió al catálogo en línea de la Biblioteca MAX Von BUCH de la Universidad de San Andrés, y a las bases de datos por suscripción: EBSCO, Proquest, JStor, Project Muse, Hein Online, Elsevier y Taylor & Francis, y de acceso abierto: DOAJ, Scielo, Dialnet, entre otras; pero, debido a lo novedoso y disruptivo de la tecnología de la

tecnología que se investiga, se ha debido recurrir a sitios de difusión tecnológica y propios de las implementaciones consideradas para obtener información actualizada.

Asimismo, se usó el gestor de bibliográfico Mendeley para buscar información científica, almacenar y organizar documentos descargados, gestionar referencias bibliografías y lectura de archivos PDF.

Las citas bibliográficas, se insertaron en el documento usando el estilo APA (American Psychological Association) 6th. Edition, mediante la extensión nativa del procesador de textos Word 2010 de Microsoft.

QUAERERE VERUM
Universidad de
SanAndrés

Capítulo 3 - Estado del arte

1 – Antecedentes Internacionales de Registros de Buques

Teniendo en cuenta que el presente trabajo se desarrolla sobre el Registro Nacional de Buques de la República Argentina; para conocer el estado del arte, en primer medida vamos a repasar las experiencias internacionales en la materia de registración de buques en particular y en forma más general, dada la similitud de la técnica registral, vamos a abordar algunos casos de sistemas avanzados de registración de bienes inmuebles que se destacan en el mundo.

Composición y características de la flota mundial.

Para el análisis de los sistemas registrales de buques, pondremos el foco en la situación de las principales flotas del mundo; para ello como primer paso, nos introduciremos en un relevamiento de la composición y características de la flota comercial de los países, que comprende los buques con tonelaje bruto mayor a las 1000 toneladas de registro, y que son los que habitualmente se utilizan en el comercio exterior.

Para ello tomaremos el informe estadístico anual 2019 de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), organismo de la Asamblea General de la ONU, cuyo objetivo es maximizar las oportunidades comerciales, de inversión y desarrollo de los países en vías de desarrollo así como la asistencia en sus esfuerzos para integrarse en la economía mundial,. Esta institución publica anualmente desde 1968, una emblemática evaluación del transporte marítimo (“The Review of Maritime Transport”), en la que proporciona un análisis detallado de los cambios estructurales y cíclicos que afectan el comercio marítimo, los puertos y el transporte marítimo en general, así como una amplia colección de información estadística.

Según este informe, a fines de 2018, la flota mundial poseía una capacidad de carga de casi 2 mil millones de toneladas de carga, distribuidos en unos 52 mil buques mayores de 1000 Tns de registro bruto; habiendo una marcado desarrollo de los buques especializados en todos los segmentos, en detrimento de los buques de carga de propósito general.

El 90 por ciento de esos buques son construidos en astilleros ubicados en China (40%), la República de Corea (25%) y Japón (25%); en tanto que los principales centros de desguace de buques se ubican en Bangladesh (46%), India (25%) y Pakistán (21%), representando el 92 por ciento del total.

En materia de economías propietarias de buques, encontramos hacia enero de 2019, que el 51 por ciento del total de propietarios se concentraban en solo cinco países: Grecia (18%); Japón (11%), China (11%), Singapur (6%) y Hong Kong (5%). De la totalidad del tonelaje mundial, compañías asiáticas son propietarias del 51%, en tanto que compañías europeas representaban el 41%, las norteamericanas el 6% y el restante 2% por ciento corresponde a empresas de América Latina y el Caribe, África y Oceanía.

Economy of ownership (Ranked by number of ships owned)	Flag of registration (Ranked by number of ships registered)							
	Panama	China	Liberia	Marshall Islands	Singapore	China, Hong Kong SAR	Indonesia	World
China	573	3 987	60	53	51	905	7	6 125
Greece	454	0	958	952	32	20	1	4 536
Japan	2 060	0	178	189	128	58	9	3 822
Singapore	257	2	152	122	1 511	131	87	2 727
Germany	32	1	673	137	70	20	0	2 672
Indonesia	17	1	7	0	7	4	2 062	2 145
Norway	54	0	85	126	95	41	4	2 038
United States of America	74	0	95	356	6	49	0	1 978
Russian Federation	35	0	130	1	2	1	0	1 707
Korea, Republic of	455	0	43	255	3	25	5	1 647
World	6 465	4 039	3 456	3 454	2 600	2 442	2 216	51 684

Ilustración 1 - Número de buques comerciales mayores de 1000TNs (UNCTAD , 2019)

En la ilustración 1, podemos ver una tabla con las principales diez economías propietarias de buques (que representan casi el 60% de la flota) y la bandera de registración que utilizan sus buques.

Se destaca que Japón por ejemplo, posee más de la mitad de su flota registrada en Panamá; China tiene un tercio de su flota radicada fuera de su bandera, principalmente en Hong Kong y Panamá. Estados Unidos, Rusia, Alemania, Noruega y Corea también tienen casi la totalidad de sus flotas registradas en banderas extranjeras, principalmente Liberia, Marshall Islands y Panamá. Singapure si bien posee más del 50% de su flota bajo su propia bandera, tiene también una parte importante de sus buques bajo banderas extranjeras. Indonesia en cambio, posee casi la totalidad de su flota bajo su propia bandera.

Los registros de buques más importantes

La mayoría de los barcos comerciales se encuentran registrados bajo una bandera que generalmente no es coincidente con la nacionalidad de la compañía propietaria del barco. No vamos a hacer una descripción detallada de las características de los distintos tipos de registros existentes, pero a modo de síntesis podemos remitirnos a la siguiente clasificación:

1. Registro Nacional (tradicional) o Cerrado: Es un registro que solo admite buques que son de propiedad de compañías o personas que poseen la nacionalidad del país. Existe una relación auténtica entre el buque, el propietario y la bandera, de modo que la nave y sus relaciones quedan sometidas a la legislación y jurisdicción de ese país. Los registros cerrados son los tradicionalmente nacionales y prácticamente todos los países poseen un registro propio.

2. Registro Internacional (clásico) o Abierto: Son registros que no tienen restricciones de nacionalidad de los propietarios para registrar un buque bajo su pabellón. El buque enarbola la bandera del país de registro y se somete a sus leyes y jurisdicción. Dentro de esta categoría de registro, se encuentran los que poseen más buques y/o tonelaje, contando actualmente con más de la mitad del registro de los buques del mundo; siendo los más importantes: Panamá, Liberia, Chipre y Honduras.

3. Registro Secundario u Off Shore: El registro secundario, o segundo registro o registro offshore; es otro registro que se abre junto a un registro cerrado y permite incorporar buques con bandera nacional pero operados por tripulaciones extranjeras.

4. Registro Especial: Los registros especiales son un híbrido entre un registro nacional y uno internacional. Tienen las características y facilidades de los registros internacionales (abiertos), pero están destinados a propietarios o armadores nacionales (cerrados). Tienden a dar facilidades para que los propietarios u armadores locales, lo consideren sobre los registros abiertos. Algunos registros, bajo ciertos requisitos, admiten armadores extranjeros, como en el caso de los registros de Noruega,

Dinamarca y Madeira (Portugal) entre otros. Los registros internacionales de Alemania y Francia, habilitan la inscripción de buques con armadores o propietarios de cualquier nacionalidad.

5. Registros del grupo “Insignia Roja” (Red Ensign Group) incluyen territorios de ultramar británicos y dependencias del GB (Naves de cualquier tipo, longitud o tonelaje): Reino Unido, Bermudas, Islas Vírgenes Británicas, Islas Caimán, Gibraltar y la Isla de Man.

Dentro de estos grupos de registros internacionales, se encuentran los que se denominan “bandera de conveniencia”. Las organizaciones sindicales los denominan de “conveniencia” porque a través de ellos los propietarios o amadores, tiende a evitar impuestos, cargas sociales y derechos de los trabajadores. En esta categoría la Federación Internacional de los Trabajadores del Transporte incluye a las siguientes banderas: Antigua y Barbuda, Bahamas, Barbados, Belice, Bermudas (Reino Unido), Bolivia, Camboya, Islas Caimán, Comoros, Chipre, Guinea Ecuatorial, Islas Faroe (FAS), Segundo Registro Internacional Francés (FIS), Segundo Registro Internacional Alemán (GIS), Georgia, Gibraltar (Reino Unido), Honduras, Jamaica, Líbano, Liberia, Madeira, Malta, Islas Marshall (Estados Unidos), Mauricio, Moldavia, Mongolia, Myanmar, Antillas holandesas, Corea del Norte, Panamá, Santo tomé y Príncipe, San Vicente, Sri Lanka, Tonga y Vanuatu.

Seguidamente analizaremos los principales registros y las características de sus sistemas administrativos en base a la información disponible:

Panamá

El Registro Naval de Buques de Panamá es un organismo estatal que se creó en 1917, cuando se establecieron los procedimientos administrativos para la nacionalización de los barcos. Es un registro Internacional y actualmente es el mayor registro de buques del mundo con unas 6465 embarcaciones, lo que representa el 12,5% de la flota mundial (UNCTAD , 2019). Un tercio de esos buques son propiedad de intereses japoneses (2060), y después se destacan por cantidad de buques, propietarios chinos (573), surcoreanos (455), griegos (554) y singapurenses entre los más importantes.

Además controla el registro y habilitación de más de 600.000 oficiales y marineros de todo el mundo, que se encuentran bajo la competencia de la legislación de ese país; por lo que no es solamente el mayor registro a nivel de buques, sino también el mayor en materia laboral. El registro de Panamá, es un registro que se ganó su reputación en la comunidad financiera internacional en base a la confianza que ha generado después de más de cien años de existencia.

La actividad en torno al registro de buques, es una de las más lucrativas del país, por eso intenta acompañar al cambiante entorno marítimo y brindar servicios de calidad para satisfacer las necesidades y demandas de sus clientes.

Su principal competencia son los registros de Liberia e Islas Marshall que son registros Internacionales, pero privados, los cuales tienen la facilidad de adecuarse más rápidamente a los cambios que requiere el mercado. El proceso de toma de decisiones panameño, al ser un registro estatal, es mucho más complejo y burocrático. (Guzmán, 2020)

La Autoridad Marítima de Panamá, está convocando a una licitación pública internacional en 2020 para la provisión del software de integración de los sistemas que actualmente utilizan la Dirección General de Marina Mercante de la Autoridad Marítima de Panamá (Registro de Buques) y la Dirección General de Registro de Propiedad Pública de Barcos (propiedad títulos y registro de hipoteca) y que se denominará "Sistema Electrónico de Registro de Buques (ESRS)”; con el cual espera simplificar los procesos de administrativos y de acceso a los usuarios distribuidos alrededor del mundo. En esta plataforma estarán disponibles los principales trámites que se efectúan ante el registro como

inscripciones de buques, registro de hipotecas y cancelaciones, gravámenes, modificaciones técnicas y de registro, reserva de nombres, etc.

“Los usuarios, armadores, operadores, gerentes, bancos y / o bufetes de abogados podrán usar la plataforma directamente. Al final, tratarán con un solo sistema. Se integrará el sistema PKI (Public Key Infrastructure), que hasta la fecha solo es por los abogados. La plataforma será versátil en diferentes idiomas. Este nuevo sistema nos posicionará en la era global". (AMP, 2019). “El ESRS ofrecerá firma electrónica: Todos los documentos serán firmados electrónicamente; esta funcionalidad implica un acuerdo con el Registro Público de Panamá y la Dirección General de Firma Electrónica. Los certificados de registro electrónico (patente de embarque, licencias de radio y otros) con QR y / o código de barras estarán disponibles para imprimir. Una pasarela de pago estará disponible con todos los diferentes métodos de pago utilizados actualmente, como tarjetas de crédito y débito. Mediante una calculadora online los usuarios podrán calcular los costos de cada operación, incluidos los descuentos. Los certificados se emitirán electrónicamente; pudiendo los usuarios solicitar y recibir sus certificaciones de propiedad y gravámenes y firmadas electrónicamente, en inglés y español. Se emitirán electrónicamente los apostillados facilitando los procedimientos de legalización ante el Ministerio de Relaciones Exteriores. Mediante una aplicación (App) para dispositivos móviles se podrán rastrear los procedimientos ejecutados y se enviarán alertas por correo electrónico a través de las diferentes etapas del proceso de registro. (AMP, 2019).

La implementación de este sistema según lo proyectado se realizará por fases y se espera que esté operando completamente a finales del 2020. Si bien no se pudo tener acceso al pliego de la licitación, se puede deducir en base a la información disponible, que el nuevo "Sistema Electrónico de Registro de Buques (ESRS)¨ si bien incorporará infraestructura de firma digital, no se hace mención a la utilización de infraestructura del tipo de blockchain, DLT o similar.

China

La norma que regula el registro de buques es el Reglamento de la República Popular de China de 1994 y las medidas provisionales para el registro de hipotecas sobre buques en construcción. Las administraciones locales de seguridad marina son las entidades gubernamentales responsables del registro de buques en China (la "autoridad de registro"). (Official Guide to Ship & Yacht Registries ("OGSR"), 2020)

El registro de buques es de carácter estatal, cerrado y los propietarios de los buques deben ser ciudadanos chinos o empresas con capital mayoritario chino y tener residencia en el territorio. Los buques de este registro no pueden adoptar doble nacionalidad, y todo buque registrado previamente en el extranjero deberá haber sido eliminado de su anterior registro, para poder ser registrado en China. La adquisición, transferencia o extinción de la propiedad de un buque se registrará en la Administración de Registro de Buques; ninguna adquisición, transferencia o extinción de la propiedad del barco actuará contra un tercero a menos que esté registrado. (Asian Legal Information Institute, 2020)

El registro Chino es el segundo en cantidad de buques a nivel mundial y posee unos 3897 buques bajo su bandera, lo que representa aproximadamente el 7,1% de la flota mundial. Sin embargo eso solo constituye dos tercios de la flota total china, ya que existen aproximadamente otros 2000 buques registrados bajo otras banderas; la mitad de ellos en el registro de la Región Administrativa Especial de

Hong Kong y el resto en otros registros abiertos del mundo. (UNCTAD , 2019). China es la economía que posee mayor cantidad de buques a nivel mundial.

Los buques de bandera china están reservados para ser tripulados por ciudadanos chinos, y en caso de ser necesario reclutar gente de mar extranjera; su empleo previamente debe ser aprobado por la autoridad competente de transporte y comunicaciones del estado. La República Popular China está adherida a la Organización Marítima Internacional (OMI) y los buques chinos en sus viajes internacionales se someten a todas las recomendaciones y resoluciones receptadas por su legislación.

La Administración de Superintendencia de Puertos de la República Popular de China es la autoridad competente encargada del registro de los buques, y posee en varios puertos agencias habilitadas y será este el puerto de registro del buque.

Recientemente la Administración de Seguridad Marítima de China y la Autoridad Marítima y Portuaria de Singapur firman un memorando de entendimiento para promover el uso bilateral y el reconocimiento de certificados electrónicos de buques entre ambas naciones; lo que nos revela que las autoridades del registro de buques chinas poseen un robusto sistema de gestión con la posibilidad de emitir certificados electrónicos basados en firma digital. (Maritime and Port Authority of Singapore, 2019).

Liberia

El Registro de Liberia es el segundo registro abierto más grande del mundo, con 3456 barcos mayores de 1000 toneladas de registro bruto, lo que representa el 6,7% por ciento de la flota oceánica mundial. El registro marítimo de Liberia es reconocido por su calidad, eficiencia, seguridad y servicio. La bandera merece la más alta consideración en la Organización Marítima Internacional y por los servicios de control de Estado Rector del Puerto, como el Servicio de Guardacostas de los EEEUU, o agrupados en memorando de entendimientos como el MOU Paris y el MOU Tokio.

El Registro de Liberia no es estatal, sino que está administrado por el Registro Internacional de Buques y Corporaciones de Liberia (LISCR, LLC), una compañía norteamericana con sede en Viena, Virginia (fuera de Washington, DC) y mantiene agencias en Nueva York, Hamburgo, Hong Kong, Leer, Londres, El Pireo, Tokio, Zúrich, Singapur y Monrovia. (Official Guide to Ship & Yacht Registries ("OGSR"), 2020). Además cuenta con amplio un staff de inspectores y auditores marítimos alrededor del mundo, lo que ayuda a su eficiencia.

Liberia fue el sitio de repatriación de los esclavos liberados en EEUU a partir de 1816, y al que comenzaron a arribar desde 1822. En 1847 se produjo la declaración de independencia de la República de Liberia. Los símbolos del Estado liberiano como su bandera, lema y escudo de armas y la forma de gobierno que eligieron reflejan su trasfondo estadounidense y la experiencia de la diáspora. (Wikipedia, 2020)

El Registro de Liberia se estableció en 1948 con el apoyo del ex Secretario de Estado de los Estados Unidos, Edward Stettinius. Desde su inicio, el Registro de Liberia ha sido operado desde los Estados Unidos, por la empresa estadounidense LISCR, LLC . El contrato entre la República de Liberia y esta empresa es, de hecho, un acuerdo estatutario, aprobado por la legislatura plena y democráticamente elegida de Liberia. La ley de Liberia requiere que los propietarios de LISCR, LLC sean ciudadanos estadounidenses para garantizar una separación entre la empresa y el gobierno de la República de

Liberia. Los cambios en el contrato / estatuto solo pueden hacerse a través de la legislación promulgada por el Gobierno de la República de Liberia. (Liberian Registry, 2020)

El registro de Liberia es la única bandera que permite el registro de doble bandera, en régimen de fletamento sin tripulación. (Liberian Registry, 2020). La economía que posee mayor cantidad de buques registrado en Liberia es Grecia, seguida por Alemania y después en menor medida los países europeos y árabes con grandes flotas. (UNCTAD , 2019). Un tercio de la flota de buques petroleros del mundo se encuentra bajo este registro.

La empresa LISCR LLC que administra el registro liberiano, también ofrece el servicio de "Operaciones Marítimas" que comprende las inspecciones de seguridad y emisión de los correspondientes certificados y de "Certificación y Documentación de La Gente de Mar" que se encarga del registro y habilitación de los tripulantes. Asimismo administra el "Registro Corporativo Liberiano" donde se inscriben las corporaciones liberianas no residentes; servicio corporativo off shore que se utiliza a la par del registro de buques.

Si bien Liberia se enorgullece de poseer uno de los registros más eficientes del mundo, para proceder a la registración de los barcos ofrece a través de una página web los formularios y procedimientos para los distintos trámites, los cuales deben ser presentados en forma física en cualquiera de las agencias que el registro posee en el mundo.

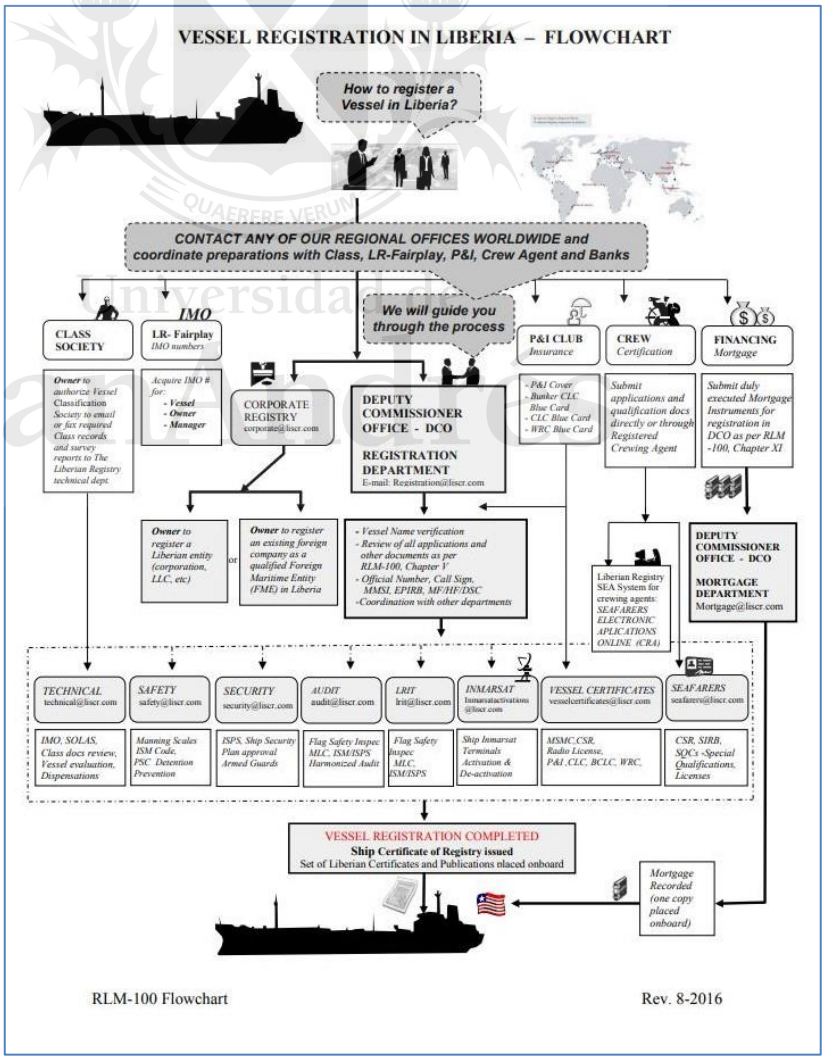


Ilustración 2 - Diagrama de flujo del registro de buques de Liberia (Liberian registry, 2020)

Por otra parte, y como el registro también administra la gente de mar; utiliza un sistema denominado "SEA System", "Sistema de Aplicación Electrónica de la Gente de Mar", aplicación basada en la web, diseñada específicamente para enviar formularios completos, documentos y que cumplen con los estándares del convenio de formación y titulación de la gente de mar de la OMI[1] (STCW). Los documentos incluyen certificados de oficial, identificación de la gente de mar y libros de registro, certificados de calificación especial y certificado de recepción de solicitud.

Para el caso de los registros de corporaciones – que se efectúan en el mismo registro – se dispone de un sistema denominado e-Corp, aplicación web que brinda acceso en tiempo real para crear nuevas empresas, reservar nombres, obtener certificados y efectuar pagos electrónicos.

Otro sistema relevante que posee el registro, es el denominado "Electronic Oil Record Book" (e-ORB); que es un sistema diseñado para reemplazar los tradicionales libros de registro de hidrocarburos que llevan obligatoriamente los buques. Usando un portal denominado "i-Sea") y mediante un servicio web basado en una nube creada con tecnologías Microsoft Azure e infraestructura de firma digital, se transmiten los datos a tierra y permite compartirlos con la tripulación, operadores y autoridades. El sistema fue desarrollado por la empresa "Prevention at Sea" radicada en Chipre.

Observamos que de los cuatro sistemas que utiliza la empresa LISCR LLC, el del Registro de Buques es el tecnológicamente menos desarrollado; ya que ofrece formularios online, que deben ser completados y presentados presencialmente en sus oficinas.

Islas Marshall

Las Islas Marshall fueron parte del antiguo Territorio Fiduciario de las Naciones Unidas de las Islas del Pacífico, bajo la administración de los Estados Unidos y en 1986, después de la firma del Pacto de Libre Asociación con los Estados Unidos, declararon su independencia.

El registro de las islas Marshall es abierto y privado, operado por International Registries, Inc. (IRI), compañía con sede en Reston, Virginia , Estados Unidos; que atiende el Registro Corporativo de las Islas Marshall en nombre de la República de las Islas Marshall. (Wikipedia, 2020)

La corporación predecesora de esta empresa fue Liberian Services, Inc., administradora del Registro de Liberia. Posteriormente esta empresa pasó a ser controlada por el Banco Internacional (IB), con sede en Washington, DC., período en el cual se expandió el Registro de Liberia.

International Registries, Inc. se formó en 1990 y firmó un acuerdo con la República de las Islas Marshall (RMI) para desarrollar un nuevo programa marítimo y corporativo. En 1993, IRI se convirtió en una empresa privada, de propiedad y operada por sus empleados senior.

Es un registro abierto, que ofrece servicios a los armadores de todas las naciones y proporciona neutralidad política, pocas restricciones relativas a la nacionalidad de la tripulación y ninguna restricción sobre dónde se construye o financia un buque. Este registro atiende también la registración y habilitación de la gente de mar. (International Registries, 2014).

[1] OMI (IMO) Organización Marítima Mundial

A principios de 2020 poseía 3454 buques mayores de 1000 toneladas; solo dos menos que el registro de Liberia; ubicándose como el segundo registro abierto y privado más grande del mundo con vistas a superar a Liberia en la primera posición a la brevedad.

Para la registración de buques; compañías y personal de la navegación, se dispone de una página web en la que se puede acceder a la totalidad de formularios y requisitos, que una vez llenados y con la documentación correspondiente se deben presentar físicamente en cualquiera de las agencias del registro distribuidas en los distintos puertos.

Si bien el registro posee un sistema informático de gestión, éste no deja de ser del tipo tradicional donde se ofrecen formularios vía web, pero necesariamente los documentos y sus adjuntos ser presentados presencialmente en las oficinas del organismo.

Singapur

El Registro de Buques de Singapur es administrado por la Autoridad Marítima y Portuaria de Singapur (MPA). Singapur es el quinto registro del mundo, tanto por tonelaje como por cantidad de barcos (2600) mayores de 1000 toneladas de arqueo. Singapur es uno de los estados más desarrollados en materia de administración marítima y portuaria.

En 1999, la Autoridad Marítima y Portuaria, lanzó su primer sistema basado en internet para operaciones marítimas, denominado MARINET. Este sistema ofrece servicios para que la comunidad naviera pueda acceder en línea, y realizar la mayoría de los servicios marítimos y portuarios, interactuando en la aplicación los organismos estatales y los operadores navieros.

A fines de 2019, la Asociación de Armadores de Singapur (Singapore Shipping Association, SSA), la Cámara de Comercio Internacional (ICC) y la start-up tecnológica Perlin, firmaron un acuerdo para el desarrollo de un sistema avanzado de registro digital de buques basado en tecnología blockchain denominado International E-Registry of Ships (IERS). Según esta misma fuente, este proyecto tiene como objetivo “racionalizar, estandarizar y mejorar drásticamente el laborioso proceso de registración de buques”, permitiendo significativos ahorros en costos de operación, tiempos de gestión, errores humanos y fraude. (Ship Technology Global, 2019)

El IERS estará desarrollado con el protocolo “Wavelet” de la empresa dinamarquesa Perlin. Utilizará tecnología blockchain, con contratos inteligentes autoejecutables. Singapur pretende ser el primer caso, banco de pruebas y definir un nuevo estándar digital para los registros de buques. (medium.com, 2020)

Como vemos, la AMP de Singapure, se encuentra trabajando con tecnología blockchain/DLT para formalizar una aplicación basada en esta tecnología y con la intención de que se convierta en un estándar para la industria marítima.

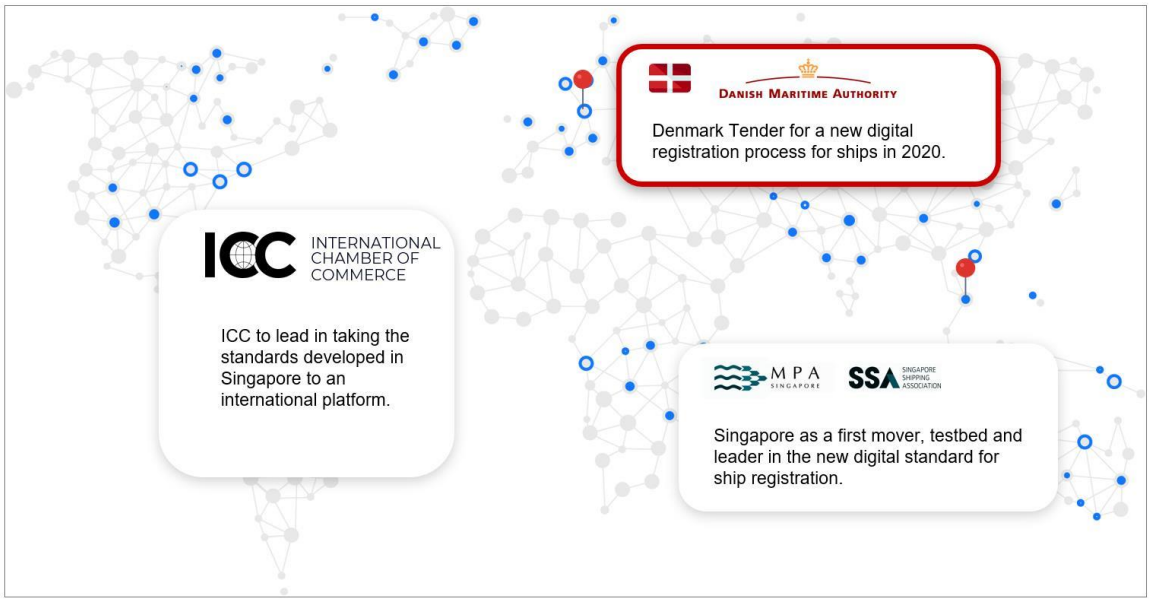


Ilustración 3 - International E-Registry of Ships (IERS) (Maikro, 2019)

Dinamarca

Si bien Dinamarca no es una de las mayores flotas del mundo, si posee una importante cantidad de buques (391), pero lo más relevante es que radica uno de los operadores marítimos más grandes del mundo: Maersk Line, que controla alrededor de 800 buques de diferentes banderas.

La Autoridad Marítima Danesa ha iniciado un proyecto que tiene como objetivo digitalizar el comercio y los procesos de registro de buques utilizando tecnología blockchain. El proyecto es parte de la estrategia gubernamental para impulsar el crecimiento digital en Dinamarca. Se espera que el proyecto comience en 2018 y se ejecute hasta principios de 2020. (Danish Maritime Authority, 2018)

"Un objetivo clave del proyecto es hacer que los procesos sean más fáciles y menos gravosos que hoy, cuando los procesos administrativos se basan principalmente en papel. El proyecto convertirá al Registro Danés Internacional de Buques en el primer registro digital de barcos del mundo. El proyecto es uno de los primeros proyectos de blockchain en el sector público danés." (Danish Maritime Authority, 2018)

En este sentido el Ministro de Industria, Negocios y Asuntos Financieros, Brian Mikkelsen expresó que "Blockchain es una tecnología avanzada con un enorme potencial para reducir las cargas administrativas. Es importante que Blue Denmark[2] en su conjunto logre desarrollar nuevas tecnologías para que podamos mantener nuestra sólida posición marítima y hacer que Dinamarca sea aún más atractiva como estado de bandera". (Safety4sea, 2018)

Experiencias en otros tipos de registros de similares características.

[2] Blue Denmark consta de armadores y compañías navieras y una gran cantidad de empresas cuyas actividades emanan del transporte marítimo internacional y danés. Son, por ejemplo, corredores de barcos, puertos y empresas de logística. Los astilleros y las empresas industriales y de servicios que suministran equipos, componentes y servicios a los buques también forman parte de Blue Denmark. (Danish Maritime Authority , 2020)

Dado lo incipiente de la tecnología blockchain aún resulta difícil encontrar proyectos implementados o en estudio concreto de ser llevados adelante en registros de buques; por lo que recurrimos a otros registros de similares características operativas y formalidades, como los registros de tierras y bienes inmuebles; para observar algunas experiencias internacionales en materia de digitalización.

Estonia

En 2007 la República de Estonia sufrió uno de los ataques de cibernéticos más grandes del mundo dirigido a sitios web de las organizaciones estonias (parlamento, bancos, ministerios, medios periodísticos, etc.) (Trustnodes, 2019). Las autoridades convocaron los científicos más prominentes de la nación y se les planteó el desafío de diseñar un sistema que permita mejorar la gobernanza de la información y de firma digital a escala masiva sin depender de autoridades de confianza centralizadas. En esas circunstancias se crea la empresa Guardtime, una iniciativa pública-privada, en la cual se desarrolla en 2008 la tecnología de 'infraestructura de firmas sin llave' (KSI), la que es publicada en 2013 en el paper denominado "Keyless Signatures Infrastructure: How to Build Global Distributed Hash-Trees" (Buldas, Kroonmaa, & Laanoja, 2013). No está fundada en la infraestructura PKI tradicional, aunque sí hace uso de criptografía y se trata de una base de datos distribuida muy eficiente con árboles de Merkle y hashes, y que ellos mismo denominan 'blockchain´ (KSI blockchain infraestructura).

Con KSI Blockchain implementada en las redes del gobierno de Estonia, se asegura la integridad y autenticidad de los datos electrónicos; impidiendo que hackers, administradores del sistema o el gobierno, puedan manipular los datos. La tecnología KSI blockchain emplea funciones hash unidireccionales para generar firmas digitales que dan pruebas tiempo, integridad y la atribución de origen de los datos electrónicos. (eEstonia, Marzo 2020).

El gobierno de Estonia dispone desde 2019 de una capa de intercambio de datos denominada X-tree (antes usaba X-Road), similar a un ESB (Enterprise Service Bus) y en el cual se basa su ecosistema de interoperabilidad, donde los miembros describen los datos compartidos y otros pueden usar estos datos en base a un acuerdo tipo SLA. (Ria, 2019).

La plataforma Guardtime KSI, es una plataforma full-stack que sigue la filosofía de Unix de abstracción y encapsulación en capas, que permite procesos federados y complejos de múltiples partes, escalan fácilmente a millones de transacciones por segundo y entienden que puede escalar más que los enfoques predominantes para blockchain/DLT, por que no necesitan para su consenso pruebas de trabajo o autoridad y ni construir un sistemas de confianza cero ya que depende de autoridades confiables. En Guardtime, se utilizan algoritmos de consenso pero para tolerancia a fallas y ataques, no como prueba de consenso. Otro punto es que posee la capacidad de dividir los libros mayores en componentes más pequeños o sub-libros de manera que se puedan validar de forma independiente y sin necesidad de que se comuniquen entre sí. (Guardtime, 2020).

Estonia fue el primer estado en desplegar la tecnología blockchain en 2012 con el Registro de Sucesiones del Ministerio de Justicia; siendo actualmente utilizada por los ministerios de Economía Relaciones y Comunicaciones, Finanzas, del Interior y Asuntos Sociales. También tienen respaldo en esta blockchain los registros de Salud, Propiedad Inmueble y Gaceta del Estado (boletín oficial). Estonia utiliza esta tecnología para garantizar la integridad de los datos y sistemas gubernamentales.

La blockchain se implementa en los sistemas del Estado a través de la Autoridad de Sistemas de Información de Estonia (RIA) que es el proveedor de servicios de autenticación interno para el

gobierno, que garantiza el acceso a la red blockchain para las agencias estatales a través de la infraestructura de X-tree. Estos organismos utilizan sus propios SDK-s (Software Development kits) y otras herramientas pre-construidas para integración de servicios. (e-Estomia, 2020)

Además de Estonia, la tecnología KSI se usa en la OTAN, el DoD de EEUU, Lockheed Martin, Boing, Ericsson (socio de Guardtime), Tellstra, SAP y GE. (eEstonia, Marzo 2020)

Japón

Según una publicación de "Asian Review" (Nikkei Inc, 2017); el gobierno japonés se encuentra desarrollando un sistema de registros de propiedad y bienes raíces basado en tecnología blockchain, que tendrá como uno de sus objetivos unificar datos en un solo repositorio y propender a la reutilización de tierras vacías o sin dueño. Esta iniciativa estaría destinada a unificar todos los registros de propiedades y terrenos en áreas urbanas, agrícolas y forestales en un solo registro basado en tecnología blockchain.

El nuevo sistema, también estaría disponible para el acceso desde el sector privado, con adecuadas medidas de seguridad y privacidad y estaría operativo en todo el país en 2022 (Property Guru, 2019).

Reino Unido de Gran Bretaña

Según la publicación "Ledger Insights" (Ledger Insights, 2019), la Oficina de Registro de Tierras del Reino Unido (HM Land Registry) dentro de su proceso de digitalización, comenzó a buscar nuevas soluciones ante la inminente necesidad de acelerar los procesos referentes a títulos de propiedad y trámites similares; y se piensa en la tecnología de DLT / Blockchain como una respuesta sumamente eficiente, con sus registros inviolables y contratos inteligentes. Con este proyecto, se espera mejorar la velocidad y la eficacia de estos procesos que aún no están digitalizadas o requieren permisos especiales de personas determinadas.

HM Land Registry (HMLR) ha seleccionado a la consultora Methods y utilizar la plataforma de blockchain CORDA/R3, para su proyecto de investigación y desarrollo llamado Digital Street. (Methods, 2018)

Conforme el informe de esta consultoría, "Digital Street es un proyecto innovador de investigación y desarrollo que tiene como objetivo involucrar a la industria para comprender cómo la tecnología de blockchain y el libro mayor distribuido pueden revolucionar el registro de tierras y el proceso de compra-venta de propiedades, haciéndolo más fácil, más rápido y más transparente".

La consultora Methods, posee varios proyectos de transformación digital con otros organismos del sector público del Reino Unido.

Suecia

En la publicación del portal electrónico Criptonoticias (Perez, Isabel, 2020) se informa que el Registro de Propiedad de Suecia, en colaboración con la empresa especializada en blockchain "ChromaWay", llevaron cabo una prueba sobre la plataforma basada en DLT que están desarrollando con el fin de agilizar el proceso de bienes raíces en el Suecia.

Los datos se resguardaron y verificaron mediante la plataforma Postchain, una blockchain privada que también admite contratos inteligentes, usada por ChromaWay. La blockchain que resguardará estos documentos se planea sea controlada por el Registro de Propiedad de Suecia, quien permitiría o no el acceso a otros actores autorizados de la industria, desde bancos hasta compradores. De esta forma, todos estarán interconectados y podrán consultar toda la historia de una propiedad por medio de una interfaz sencilla.

Como resultado del test; se observó la necesidad de aplicar métodos de identificación de los actores más rígidos (como por ejemplo biométrico) y atender los aspectos legales y regulatorios dado que existe cierta incertidumbre legal sobre si las firmas que no estén en papel tendrán validez, aunque su aceptación ha comenzado a extenderse en Europa.

República de Georgia

A través de la consultora a Bitfury, se implementó el sistema de registro de tierras de la Agencia Nacional de Registro Público (NAPR) de la República de Georgia, con el objetivo de fortalecer los derechos de los propietarios, aumentar la confianza de los ciudadanos en el gobierno y reforzar la seguridad de los datos. (SmartDegrees News, 2020)

El proceso de registro de propiedades digitales en Georgia se basa en un servicio de marca de tiempo con Exonum de Birfury añadido al proceso. Con la característica de marca de tiempo de Exonum en el registro de títulos de tierra, NAPR pudo proporcionar a los ciudadanos georgianos certificados digitales de sus activos, respaldados por una prueba criptográfica (hash). Ese hash es publicado en Bitcoin Blockchain; permitiendo al propietario del documento probar su legitimidad.

Al integrar con éxito la tecnología blockchain en su propio registro de propiedad, el gobierno georgiano ha dado por concluido el primer paso de la tecnología pionera de blockchain. La misma tecnología también se implementará en todos los registros gubernamentales de la República de Georgia. El proyecto continuará avanzando incluyendo posibilidades de un contrato inteligente para agilizar las operaciones comerciales de NAPR, incluyendo la venta de propiedades, la transferencia de la propiedad y más. (Bitfury, 2020)

Existen otras iniciativas similares en el mundo; particularmente España, Brasil e India entre otros países, que están considerando la utilización de tecnología blockchain/DLT para brindar seguridad y transparencia en sus registros públicos; y si bien estas experiencias no serán tratadas en el presente trabajo, es suficiente para advertir que la tecnología blockchain/DLT está siendo aplicada y experimentada intensamente para su utilización en registros de buques y similares.

2 - Aspectos Tecnológicos

Introducción a Blockchain/DLT

Blockchain o "cadena de bloques" básicamente una base de datos distribuida de registros, una analogía digital de un libro mayor en el que todas las transacciones son realizadas y compartidas entre los participantes de la red informática. Cada transacción en este registro o libro mayor púbico se verifica por consenso de la mayoría de los participantes en el sistema y una vez que la transacción es confirmada por la mayoría, nunca más podrá ser borrada o alterada. Así, blockchain contiene un registro cierto, verificable e inmutable de cada transacción que ha sido realizada.

Blockchain o más ampliamente, Tecnología de Contabilidad Distribuida ("DLT Distributed Ledger Tecnology) , es una tecnología que permite la realización confiable y segura de cualquier tipo de transacción entre dos o más personas sin la necesidad de intermediarios, a través de Internet. Su introducción al mundo se dio a través de la criptomoneda Bitcoin, la primera plataforma blockchain. Originalmente, Bitcoin se creó como un sistema electrónico de pago entre pares (A Peer-to-Peer Electronic Cash System), por lo que se le conoce como "dinero digital".

Blockchain es una articulación de tecnologías estructuradas en un sistema naturalmente encriptado, lo que proporciona a los usuarios involucrados protección de sus identidades y de los datos de sus transacciones.

Lo que puede considerarse una innovación de blockchain, es que permite registrar transacciones de tokens. Los tokens pueden representar diferentes activos digitales, según el contexto en que se los emplee. Su denominación viene de la numismática, donde se alude a la ficha metálica que se usa como soporte para la acuñación de monedas. Es decir es un objeto susceptible de adquirir valor.

Entonces, al token le podemos dar diversos usos y representaran un valor según el contexto en que se empleen. Un token, podrá ser una ficha en un casino, un cospel que habilita un determinado juego, una ficha en un sistema de boletería, etc. En el mundo digital, los tokens representan activos digitales. Un activo digital es "cualquier recurso que existe de forma digitalizada y que alguien puede poseer, o que representa contenido que alguien puede poseer, y por tanto, tienen asociado un derecho para su uso" (Eileen Gardiner, 2015). Al ser tratados como una propiedad, esta puede venderse, comprarse o licenciarse (Koonce, 2016). Es decir, Koonce nos señala que un archivo de música adquirido de forma legítima es un activo digital; mientras que una copia ilegal carece del derecho para usarlo y por lo tanto no puede ser considerado archivo digital, aun cuando el poseedor pueda tener la habilidad para obtenerlo y ejecutarlo. Los derechos digitales, típicamente están embebidos en los metadatos del archivo; de manera homóloga al título de propiedad que acompaña un bien inmueble y mueble registral, y permite ser transferirlo.

Los tokens son cadenas alfanuméricas que representan un registro en la base de datos descentralizada de consenso. Todas las criptomonedas, independientemente de sus características técnicas, son tokens que funcionan como medios de intercambio (aunque también se les puede dar otras utilidades); y debido a que generalmente son emitidos por empresas privadas, instituciones, asociaciones o personas, no es dinero de curso legal.

Otras de las características de blockchain, es que ha demostrado ser invulnerable, y esta propiedad se funda en que está completamente distribuido y es actualizado constantemente con las nuevas

transacciones, que al irse incorporando van 'sepultando' las transacciones anteriores haciendo cada vez más difícil su alteración. Un gran número de transacciones se agrupan en un bloque antes de escribirse en ese gran libro mayor que es blockchain. Cualquier entidad participante puede registrar transacciones en blockchain, pero que una vez escrito no hay forma que pueda borrase o modificarse, si bien todos pueden leerlo.

Esta base de datos distribuida que es blockchain, tiene estas características esenciales:

- Única fuente de confianza compartida (no necesita de terceros de confianza)
- Inmutable
- No falsificable

Como vimos, todas las transacciones se anotan en un "libro de contabilidad digital", agrupadas en bloques que continuamente son enlazados linealmente entre sí, es decir el primer bloque con el segundo, el segundo con el tercero, y así sucesivamente (de allí el nombre de 'cadena de bloques'). Esa cadena acumula el registro histórico de todas las transacciones anteriores, impidiendo de esta forma el "doble gasto"[3], evitando que un valor digital pueda usarse más de una vez, ya que la transacción se encuentra registrada en un libro contable de libro acceso.

Cuando se crea un bloque, las transacciones contenidas en él tienen un nivel de confirmación. Cuando se crea el siguiente bloque tienen dos, y así sucesivamente va incrementando su nivel de confirmación. Se entiende que cuando acumula seis niveles, la transacción es definitivamente irrevocable y verificable. Bitcoin, que es la primera implementación de Blockchain, ha funcionado perfectamente a lo largo de los años.

La economía digital actual se basa en la dependencia de una cierta autoridad de confianza. El hecho es que en el mundo digital una tercera entidad para la seguridad y privacidad de nuestros dispositivos digitales pueden ser hackeada, manipulada o comprometida y es aquí donde la tecnología blockchain se destaca. Tiene el potencial de permitir un consenso distribuido donde cada transacción en línea que involucre activos digitales pueda ser verificada en cualquier momento, sin comprometer la privacidad de los activos digitales o las partes involucradas. El anonimato y el consenso distribuido son dos de las principales propiedades de blockchain.

Un caso de uso típico de blockchain, es la prueba de existencia de un activo digital, ya sea éste un documento legal, un título mueble o inmueble, un registro de salud, pagos, etc. La prueba de existencia indica la existencia de un archivo de computadora en un momento específico mediante una marca de tiempo en un registro en la cadena de blockchain.

Otro caso de uso emergente de la tecnología blockchain corresponde a los "contratos inteligentes", que son básicamente programas informáticos que pueden ejecutar automáticamente los términos de un contrato dentro de una cadena de blockchain. Cuando una condición prestablecida en un contrato inteligente se cumple, entonces se ejecutan automáticamente y de manera transparente las acciones pre acordadas en el contrato.

[3] El doble gasto es un defecto potencial del dinero digital por el que una misma moneda digital (a la que también se llama token) puede gastarse más de una vez. Esto es posible porque cada moneda consta de un archivo digital que puede duplicarse o falsificarse (Ryan, 2017.)

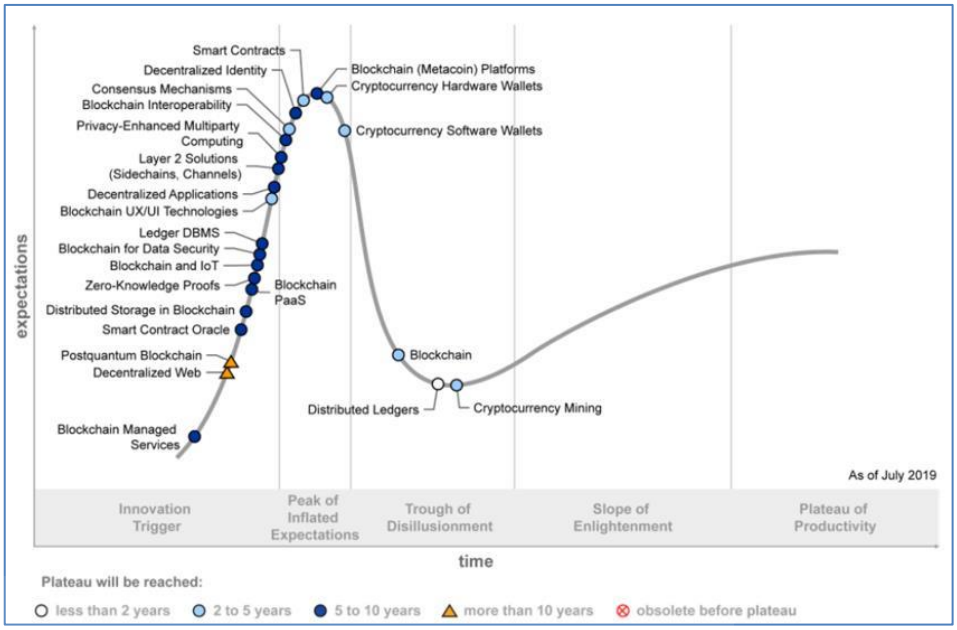


Ilustración 4 - Gartner - Hype Cycle for Blockchain Technologies, 2019 (Gartner, 2019)

El informe de Gartner (Gartner, 2019) que publica el Hype Cycle de Gartner 2019, muestra que la mayoría de las tecnologías blockchain aún están a 5 o 10 años de distancia del impacto transformador. Las tecnologías Blockchain se están deslizando hacia el valle de la desilusión, del que comenzará a salir hacia 2021, en la medida que la tecnología avance y los casos de uso pragmáticos con el soporte exclusivo de blockchain continúen desplegándose. El canal de la desilusión destaca las tecnologías y los mercados en los que el interés ha disminuido a medida que los experimentos y las implementaciones no se entregan.

Avivah Litan, VP de investigación de Gartner sostiene que: "Las tecnologías Blockchain aún no han estado a la altura de las expectativas y la mayoría de los proyectos empresariales de blockchain están estancados en modo de experimentación. Blockchain aún no permite una revolución comercial digital en los ecosistemas empresariales y puede que no sea hasta al menos 2028, cuando Gartner espera que blockchain se vuelva totalmente escalable técnica y operativamente". (Litan, Avivah, 2019)

Según el informe de Gartner, para que blockchain/DLT se convierta en la corriente principal, los usuarios no deberían tener que preocuparse por elegir la plataforma correcta, el lenguaje de contrato inteligente correcto, las interfaces de sistema correctas y los algoritmos de consenso correctos. Además, las preocupaciones sobre cómo los usuarios interactuarán con socios que usan diferentes plataformas de blockchain para sus proyectos deben ser rectificadas.

“Estamos presenciando muchos desarrollos en la tecnología blockchain que cambiarán el patrón actual. Para 2023, las plataformas blockchain serán escalables, interoperables y admitirán la portabilidad de contratos inteligentes y la funcionalidad de cadena cruzada. También admitirán transacciones privadas confiables con la confidencialidad de datos requerida. Todos juntos, estos avances tecnológicos nos llevarán mucho más cerca de la cadena de bloques convencional y la web

descentralizada, también conocida como Web 3.0. Con el tiempo, las cadenas de bloques autorizadas se integrarán con las cadenas de bloques públicas, y aprovecharán los servicios compartidos mientras respaldan los requisitos de membresía, gobierno y modelo operativo de las cadenas de bloques autorizadas", agregó la Sra. Litan. (Litan, Avivah, 2019)

Diferencia entre Blockchain y DLT (Distributed Ledger Technology)

Un libro mayor distribuido es una base de datos que se extiende a través de varios nodos o dispositivos informáticos. Cada nodo se replica y guarda una copia idéntica del libro mayor. Cada nodo participante de la red se actualiza de forma independiente. La característica innovadora de la tecnología de contabilidad distribuida es que ninguna autoridad central mantiene la contabilidad. Las actualizaciones del ledger son construidas y registradas de forma independiente por cada nodo. Los nodos luego votan sobre estas actualizaciones para asegurar que la mayoría esté de acuerdo con la conclusión alcanzada. Esta votación y acuerdo sobre una copia del libro de contabilidad se denomina consenso y se realiza automáticamente mediante un algoritmo de consenso. Una vez que se ha alcanzado el consenso, el libro mayor distribuido se actualiza por sí mismo y la última versión acordada del libro mayor se guarda en cada nodo por separado. Las tecnologías de libro mayor distribuido reducen drásticamente el costo de la confianza. Las arquitecturas y estructuras de los libros de contabilidad distribuidos pueden ayudarnos a mitigar nuestra dependencia de los bancos, gobiernos, abogados, notarios y funcionarios de cumplimiento normativo.

Las cadenas de bloques (blockchain) son una forma de tecnología de contabilidad distribuida (DLT), pero no todas las DLT emplean una blockchain para proporcionar un consenso distribuido seguro y válido. Una cadena de bloques se distribuye y se gestiona mediante redes de igual a igual. Dado que es un libro mayor distribuido, puede existir sin una autoridad centralizada o un servidor que lo administre, y la calidad de los datos puede mantenerse mediante la replicación de la base de datos y la confianza computacional. Sin embargo, la estructura de la cadena de bloques es lo que la diferencian de otros tipos de libros de contabilidad distribuidos o DLT. Los datos en una cadena de bloques se agrupan y organizan en bloques, que luego se vinculan entre sí y se aseguran mediante criptografía.

Un blockchain es esencialmente una lista creciente de registros. Su estructura solo permite agregar datos a la base de datos: es imposible alterar o eliminar los datos ingresados previamente en bloques anteriores. Por lo tanto, la tecnología Blockchain es muy adecuada para registrar eventos, administrar registros, procesar transacciones, rastrear activos y votar. Criptomonedas, como Bitcoin, es la tecnología pionera de blockchain.

Como dijimos, todas las blockchain son libros de contabilidad distribuidos, pero no todos los libros de contabilidad distribuidos usan blockchain. En ambos casos se requiere de sistemas descentralizados y mecanismos de consenso entre los nodos; pero la cadena de bloques organiza los datos en bloques y actualiza las entradas utilizando una estructura de solo apéndice.

Trilema[4] de la tecnología blockchain

[4] Un trilema es una elección entre tres opciones, que son (o aparentan ser) contradictorias entre sí, o bien, conducen aparentemente a resultados distintos. Un trilema se puede expresar de dos formas lógicamente equivalentes: como una elección entre tres opciones contradictorias en la que solo se puede elegir una, o como

"El trilema de la escalabilidad", un término acuñado por Vitalik Buterin (fundador de Ethereum), se refiere a las concesiones que los proyectos criptográficos deben realizar al decidir cómo optimizar la arquitectura subyacente de su propia cadena de bloques. En términos sencillos, es similar a la frase 'no se puede tener todo'. El trilema al que se refiere Vitalik involucra tres componentes: descentralización, seguridad y escalabilidad" (Viswanathan & Shah, 2018).

Estos tres elementos fundamentales de blockchain, son el eje de su infraestructura y como podemos ver, existe tensión entre ellos.

Descentralización: La descentralización es el principio central sobre el cual se construye la mayoría de esta comunidad. La descentralización permite la resistencia a la censura y permite que cualquiera pueda participar en un ecosistema descentralizado sin prejuicios.

Escalabilidad: La escalabilidad se refiere a la capacidad de procesar transacciones en cualquier red dada. Si las transacciones públicas deben poder ser utilizadas por las masas, entonces deben ser capaces de manejar un escenario en el que hay millones de usuarios en la red.

Seguridad: La seguridad se refiere a la inmutabilidad del libro mayor y su resistencia general a ataques, como ataques del 51%, ataques de Sybil, ataques DDoS, etc.

Actualmente, las principales blockchain (Bitcoin y Ethereum) se diseñaron con un enfoque en la descentralización y la seguridad. Sin embargo, esto se ha producido a expensas de la escalabilidad, ya que ambos blockchain tienen tiempos de procesamiento de transacciones increíblemente lentos. La razón de esto es que todos los nodos completos en estas cadenas de bloques respectivos deben alcanzar un consenso antes de que se puedan procesar las transacciones.

"Ethereum puede procesar alrededor de 15 transacciones por segundo, mientras que Bitcoin puede procesar solo alrededor de 7 transacciones por segundo. Sin embargo, estos dos números están empequeñecidos por el servicio de pago VISA, que puede manejar hasta 24.000 transacciones por segundo. Incluso las propuestas hechas para abordar la escalabilidad de blockchain caen nuevamente sobre las cuestiones planteadas por el trilemma de escalabilidad" (Bitcoinist, 2018)

Principales características de blockchain/DLT

Si bien las blockchain/DLT fueron concebidas para ser un gran libro de contabilidad completamente público y sin restricciones de acceso para cualquiera, el devenir tecnológico y la necesidades que surgen de los casos de uso que requieren distintas entidades públicas o privadas, ha llevado a que surjan diferentes categorías o tipos según sus características particulares.

La gran diferencia entre las blockchain está relacionada con quien tiene acceso a participar en la red, el protocolo de consenso y el mantenimiento la cadena de bloques.

Blockchain públicas (Permissionless)

Una red de blockchain es pública cuando es completamente abierta y cualquiera puede unirse y participar en la red. Bitcoin es la blockchain pública más grande en producción. Las decisiones en las blockchain públicas suceden con varios mecanismos de consenso descentralizados como Prueba de Trabajo (Proof of Work - PoW), Prueba de Estado (Proof of Stake - PoS), etc. Los protocolos de blockchain públicos, del estado del arte, basados en algoritmos de consenso son open source y sin

---

un problema con tres proposiciones aparentemente favorables pero en la que solo dos son posibles al mismo tiempo

permisos; por lo tanto cualquiera puede descargarse el código y empezar a correr un nodo público en sus dispositivos locales, validando transacciones en la red; de este modo participan en el proceso de consenso que es el procedimiento para determinar qué bloques son añadidos a la cadena y su estado actual. Cualquiera en el mundo puede enviar transacciones a través de la red y esperar que sean incluidos en la blockchain si son válidas. Cualquiera puede verificar las transacciones en el explorador de transacciones públicas. Las transacciones son transparentes, pero anónimas o pseudo-anónimas. (Ejemplos: Bitcoin, Ethereum, Monero, Dash, Litecoin, etc.)

Blockchain permite eliminar la intermediación, ya que hay acciones que incluso los desarrolladores no tienen autoridad para hacer. Tampoco hay que afrontar costos de infraestructura, ya que no hay necesidad de mantener los servidores o administradores de sistemas, lo que reduce los costos de crear y mantener aplicaciones descentralizadas (dApps)

Una de las debilidades de las blockchain públicas, es que es necesaria una gran cantidad de proceso computacional para mantener un libro mayor distribuido a gran escala. Específicamente, para alcanzar el consenso, cada nodo de la red debe resolver un acertijo criptográfico complejo, mediante fuerza bruta haciendo uso intensivo de recursos (energía y refrigeración), para asegurarse que todos los nodos se mantengan sincronizados. Otra desventaja de las cadenas de bloques sin permisos, es que implica que no haya privacidad para las transacciones; lo que incomoda a las empresas y las personas.

Blockchain privadas (Permissioned)

Una red blockchain privada requiere de una invitación, que debe ser validada por el creador de la red o por un grupo de reglas puestas en marcha cuando se creó la red. Las empresas que lanzan una blockchain privada, normalmente lo hacen con una red con permisos, con el fin de poner restricciones en quién puede participar en la red y realizar transacciones. El mecanismo de control de acceso puede variar. Pueden ser los participantes quienes decidan futuros ingresantes o una autoridad reguladora quien otorgue las licencias para participar. Una vez que una entidad se ha unido a la red, jugará un rol en mantenimiento de la blockchain. Los permisos de escritura se mantienen centralizados y los de lectura pueden ser públicos o restringidos. Por ejemplo, las aplicaciones que pueden hacer uso de este modelo, son aquellas que necesitan la tecnología solamente para ellas mismas y que por tanto, tener permisos de escritura privados y de lectura públicos o restringidos. En algunos casos la auditoría pública es deseada; y ahí es donde las blockchain privadas son una manera de tomar ventaja de esta tecnología, permitiendo que solo determinados participantes puedan verificar transacciones internas. Al estar los permisos de lectura restringidos, se proveen un gran nivel de privacidad. Las blockchain con permisos, también permiten mejorar escalabilidad en términos de rendimiento en las transacciones.

Blockchain federadas o de consorcio

Este tipo de blockchain intenta eliminar la completa autonomía de una sola entidad sobre una blockchain. Básicamente, en este tipo de redes hay un grupo de empresas o de individuos que se congregan para tomar mejores decisiones para toda la red. Estos grupos son llamados consorcios o federaciones. Las blockchain federadas operan bajo el liderazgo de un grupo.

Al contrario de las blockchain públicas, en las blockchain federadas solo algunos nodos participan del proceso de verificar transacciones. Las blockchain federadas son más rápidas (más escalabilidad) y proveen de más privacidad en las transacciones. El proceso de consenso es controlado por un grupo de nodos preseleccionados. Por ejemplo, uno grupo de empresas financieras conforman una blockchain federada. Cada institución posee un nodo validador. El consorcio determina que para que un bloque

sea válido, por lo menos dos tercios de los nodos deben haber firmado el bloque. El derecho a leer la blockchain puede ser público o restringido a los participantes.

Bases de Datos Centralizadas, Descentralizadas y Distribuidas

Las bases de datos centralizadas son aquellas que mantienen todos los datos en una única computadora, ubicación y para acceder a la información se debe ingresar a la computadora principal del sistema, conocida como "servidor".

Por lo tanto, una base de datos descentralizada consiste en una serie de computadoras y servidores que se encuentran en distintos lugares geográficos, los datos no se almacenan en un solo lugar, sino que están almacenados en una serie de servidores distintos que proveen de información a los clientes.

Y una base de datos distribuida funciona como una única base de datos lógica que está instalada en una serie de computadoras (nodos) ubicadas en diferentes lugares geográficos y que no están conectadas a una única unidad de procesamiento, pero si están totalmente conectadas entre sí a través de una red de comunicaciones.

Las blockchain/DLT usan bases de datos distribuidas en la que la información está almacenada por todos los nodos que soportan esta red. Existen dos características que realmente diferencian a blockchain del resto de bases de datos: el control de acceso de escritura y lectura de datos está verdaderamente descentralizado y tienen la capacidad de asegurar transacciones sin necesidad de terceros de confianza en un entorno competitivo.

Algoritmos de consenso

La tecnología blockchain permite construir base de datos estructuradas en bloques que almacenan todos los cambios de información, pero para evita organizar las relaciones de confianza en base a un ente central, se necesita de un mecanismo de consenso de confianza que lo reemplace (Rodriguez, 2018).

Un mecanismo de consenso es una forma de llegar a un acuerdo de ciertos principios y funcionalidades que serán comunes para todos. Existen varias alternativas para los mecanismos o algoritmos de consenso; y previo a ver los más populares, es importante entender que no existe un método para alcanzar consenso de forma universal; ni un algoritmo que sea mejor que otro, ya que todo depende de los requerimientos del sistema.

El proceso de armar un bloque de transacciones y sumarlo definitivamente en la cadena se llama validación mediante el sellado o minado del bloque; y cuando esto ocurre el bloque pasa a formar parte de la cadena de forma permanente, inmutable e inalterable.

El protocolo de consenso es el mecanismo que regula la forma en que los nodos que sellan bloques llegan a un acuerdo entre sí para poder hacerlo e incorporar ese bloque a la cadena. Una vez que una transacción ingresa a la cadena de bloques es verificada y asegurada por un mecanismo de consenso tal que es extremadamente difícil alterarla.

Los algoritmos de consenso son uno de los aspectos más importantes para las blockchain públicas. Los más conocidos son la prueba de trabajo que utilizan las principales criptomonedas y los de prueba de participación basados en protocolos tolerantes a fallas bizantinas (BFT) desarrollados para sistemas distribuidos anteriores a blockchain.

Los tipos de algoritmos de consenso, más usados son:

Prueba de Trabajo (PoW)

Como su nombre lo indica, este algoritmo de consenso requiere la realización de algún tipo de trabajo. Este trabajo consiste en encontrar la solución de una compleja operación matemática, que demanda cierto costo computacional por parte del nodo y pueda ser fácilmente verificado por parte de los restantes nodos de la red. Cuanto más trabajo se realice, mayor será la probabilidad de proponer el próximo bloque en la cadena, y obtener la recompensa. También impone límites a las acciones en la red, debido a que el esfuerzo necesario de potencia computacional y tiempo para hacer los cálculos provoca que un ataque eficiente sea posible, pero inútil ya que los costos son demasiado altos, lo que previene que el sistema sea atacado creando falsos votantes.

La prueba de trabajo, es considerado el algoritmo más sencillo y al mismo tiempo el más sostenible; pero no es el más rápido ni el más eficiente; ya que requiere una enorme cantidad de esfuerzo computacional, que si bien garantizan la seguridad de la red, no es aplicable en ningún otro lado y por lo tanto se desperdicia. Para tener más probabilidades de ganar, los usuarios buscaran permanentemente realizar una mayor cantidad de trabajo, por lo que se requiere tener el mayor poder computacional, lo que ha llevado a una intensificación en la competencia por mejorar los recursos, dando origen a granjas o pool de servidores, ya que la minería de datos requiere hardware informático altamente especializado, con los ingentes costos asociados de energía en el uso de los procesadores y la refrigeración.

Tolerancia a Faltas Bizantinas (BFT)

Estos algoritmos tienen como objetivo principal alcanzar el consenso dentro de un grupo pequeño de nodos y tiene sentido cuando todos los participantes en el proceso se conoce entre ellos y no son propensos a cambiar.

Los sistemas distribuidos experimentan distintos tipos de fallas, que pueden estar relacionados con problemas internos de los elementos de la red, latencia en la comunicación o comportamientos arbitrarios de algunos de los participantes. Estas últimas se denominan fallas bizantinas, y ocurren cuando alguno de los elementos de la red actúa maliciosamente. Recibe esta denominación por el problema de los generales bizantinos [5] y es un campo de estudio enfocado a diseñar sistemas tolerantes a fallas bizantinas, fundamentalmente cuando la red tiene un funcionamiento descentralizado como en el caso de los sistemas distribuidos.

En general estos sistemas se basan en la elección de algunos nodos rotativos que actuarán bajo determinadas condiciones, como los únicos proponentes de las transacciones, mientras los demás participantes en forma directa o delegada se limitarán a votar para llegar a una mayoría de consenso que permitirá aceptarlas o rechazarlas.

Al separarse la elección de los nodos validadores, del procesamiento de validación de las transacciones, se logra que los sistemas ganen en rapidez en el procesamiento de las transacciones y no tengan el problema de escalabilidad que afecta los sistemas basados en prueba de trabajo.

El problema que impide la utilización de este tipo de protocolos en las blockchain públicas, es que para designar a los nodos validadores con anticipación, es necesario conocer de antemano a los participantes; por lo que se puede decir que la red no es completamente abierta.

[5] El problema de los generales bizantinos es un planteo que representa los problemas de comunicación que pueden ocurrir, cuando a partir de una estructura jerárquica, se intenta encontrar un plan de acción común y evitar fallos, aun cuando alguno de los participantes no sea fiable y provea información falsa de forma intencionada.

Además puede existir fraude con usurpación de identidades en un proceso que se conoce como "ataque sibil" (Douceur, 2002) de modo que un participante podría multiplicar su poder de voto y maliciosamente influir en la red.

La latencia en la red puede llegar a ser importante, si para alcanzar el consenso de la mayoría se requieren de varias rondas de comunicación entre los nodos; lo que suele ocurrir cuando la cantidad de participantes es alta.

Acuerdo Bizantino Federado (FBA)

FBA (por sus siglas en inglés) fue inicialmente utiliza por Ripple[6] y luego mejorado por Stellar[7]. El mecanismo permite alcanzar consenso entre un gran número de participantes, cuyo total se desconoce. Cada participante elige confiar en un limitado número de personas, grupo, de otros participantes, formando lo que se conoce como un círculo de confianza en donde se alcanza fácilmente el consenso. Eventualmente algún participante de un grupo tiene confianza con el de otro, haciendo que sea posible el consenso en toda la red.

Prueba de Participación (PoS)

El protocolo de Prueba de Participación - en inglés se lo denomina (Proof of Stake - PoS)-, es un protocolo de consenso para redes distribuidas que asegura una red de un moneda digital mediante la petición de pruebas de posesión de dichos activos. La cadena de bloques mantiene el registro de validadores, y quien tenga activos de esa criptomoneda en la cadena de bloques es potencialmente un validador al depositar sus activos mediante una transacción especial. La creación y aceptación de nuevos bloques se realiza entonces mediante el algoritmo de consenso, pudiendo participar todos los validadores registrados. La probabilidad de minar un bloque de transacciones y hacerse de la recompensa es directamente proporcional a la cantidad de activos que se tiene acumulado en el depósito.

El concepto subyacente es que quienes poseen más unidades acumuladas de una moneda digital son quienes más apuestan por esa moneda y en consecuencia los más interesados en preservarla y del buen funcionamiento de la red que otorga valor a sus activos; por eso también tienen mayor derechos a comprometerse con la responsabilidad de proteger al sistema de posibles ataques. Esto se logra dado que el protocolo está diseñado para ofrecer menor dificultad para encontrar bloques, a los mineros que demuestren poseer mayor cantidad de monedas en depósito.

Una de las ventajas de PoS, es que sin resignar seguridad, genera menor riesgo de centralización de la red en manos de mineros con gran capacidad de cómputo pero sin mayor interés en el destino de la moneda; a la vez que es de mayor eficiencia energética.

La desventaja de PoS es que resulta difícil construir un sistema que considere todos los posibles escenarios donde pueda haber comportamiento malicioso y también es teóricamente posible un ataque del 51%, aunque no tenga mucho sentido para los atacantes.

Prueba de Participación Delegada (DPoS)

La prueba de participación delegada DPoS (por sus siglas en inglés) consiste en que los participantes delegan en usuarios respetados de la comunidad en que participan la facultad para aprobar las transacciones. Los delegados son elegidos por los demás participantes mediante voto y sus identidades

[6] Ripple, hoy XRP Ledger o simplemente XRP es un proyecto de software libre y un protocolo de pagos que persigue el desarrollo de un sistema de crédito basado en el paradigma peer-to-peer. (Wikipedia).

[7] Stellar es un protocolo de código abierto para el intercambio de valores, que es apoyado por una organización sin fines de lucro, la Stellar Development Foundation. La misión de la Fundación es expandir el acceso financiero y la alfabetización en todo el mundo. (Wikipedia)

son bien conocidas. En la votación para elegir delgados, tienen mayor peso e influencia en la votación los participantes que cuenten con más monedas en la blockchain.

En este sistema, solo hay una cantidad limitada de validadores, lo que implica mayor velocidad para aprobar transacciones; haciendo al sistema capaz de competir eficazmente para resolver necesidades de organizaciones que necesitan una alta tasa de validaciones por segundo, como es el caso de las tarjetas de crédito. De esta manera DPoS, resuelve el problema de la escalabilidad que presentan algunos de los algoritmos.

La desventaja de este algoritmo, es que la escalabilidad se logra comprometiendo el principio de descentralización, debido a que solo un número limitado de participantes pueden validar las transacciones, lo cual resulta una amenaza ya que pueden comportarse como un ente central.

Prueba de Autoridad (PoA)

En el mecanismo de consenso de Prueba de Autoridad (PoA), existen una cantidad predeterminada de nodos que tienen permisos para agregar nuevos bloques; los que se seleccionan en base a la certeza que se posee sobre su identidad, corroborada previamente y fehacientemente con documentación emitida oficialmente para esa persona de existencia física o jurídica

Este es un modelo liviano, ya que los nodos selladores al estar predeterminados, no necesitan tener una gran capacidad de cómputo para resolver algoritmos complejos, y en consecuencia son muy eficientes energéticamente.

Debido a que no hay recompensa económica por la participación en el proceso de agregación de nuevos bloques, generalmente estos modelos no se usan para criptomonedas, ya que esa recompensa es la única manera a crear nueva moneda, y eso está perfectamente calculado desde la implementación.

Los nodos selladores, únicos habilitados para crear nuevos bloques, además de revelar fehacientemente su identidad, deben ser aceptados previamente por votación de la mayoría de los nodos selladores ya establecidos, lo que le brinda el control total sobre qué nodos serán selladores en la red. Además, para evitar que un nodo sellador pueda malintencionadamente provocar daños a la red, una vez que sellan un bloque, los nodos selladores no pueden agregar bloques consecutivos, usándose para eso distintas reglas de contención.

Asociar la identidad con el nodo, significa que los beneficios que se obtienen de él son públicos y también lo son las acciones nefastas que se podrían emprender. La identidad puesta en juego puede servir como un gran ecualizador, entendida y valorada por todos los actores.

Aun cuando el protocolo de consenso de PoA, carece de la descentralización que pregona el modelo de blockchain, se deben ponderar las ventajas ofrece la mayor eficiencia en los tiempos de transacción, lo que aumenta enormemente su escalabilidad.

Redes Centralizadas, Descentralizadas y Distribuidas

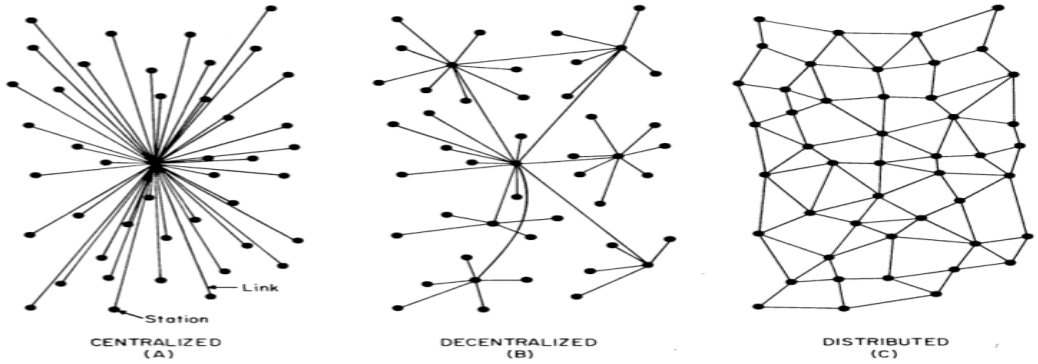


Ilustración 5 - Redes Centralizadas, Descentralizadas y Distribuidas (Baran, 1964)

Tipos de redes: centralizada, descentralizada, distribuida, P2P y cripto.

Red centralizada

En una red centralizada, existe un nodo central y varios periféricos, es decir sólo se pueden comunicar entre ellos a través del nodo central y sus canales. El flujo de comunicación se interrumpe si el nodo central sale de servicio. Es la topología es la más utilizada, sin embargo gracias a las mejoras en las redes y dispositivos que permiten una interconectividad creciente, paulatinamente están siendo sustituidas por las redes descentralizadas y distribuidas. Un clásico ejemplo de red centralizada es la red telefónica fija, donde dos abonados solo se pueden comunicar pasando por la central.

Red descentralizada

En una red descentralizada no existe un único nodo central, hay varios centros de conexión. Cuando uno de los centros de conexión se cae, se produce la desconexión de uno o varios nodos del conjunto de la red. Si cae el nodo centralizador produce obligatoriamente la ruptura y desaparición de toda la red. Es decir, los nodos se conectan entre sí, sin que tengan que pasar obligatoriamente por uno o varios centros. La red no cae ante la caída de nodos. La red descentralizada se rige por el principio de adhesión o participación.

Red distribuida

La red distribuida carece de centro individual o colectivo. Los nodos se unen uno a otro, sin que ninguno de ellos tenga el poder de filtro de los mensajes que se transmiten en la red. Si cae algún nodo, no desconecta a ningún otro, sólo él se ve afectado. La red se rige por el principio de la interacción, cada nodo es independiente y puede moverse libremente.

Internet es la clásica red distribuida, donde los nodos se pueden conectar libremente con cualquier otro. Ante la caída de un nodo de conexión la red puede redirigir los mensajes a través del establecimiento de la conexión con otro nodo operativo, y así llegar al nodo de destino.

Redes Peer-to-Peer (P2P)

“Un sistema Peer-to-Peer es un sistema auto-organizado de entidades iguales (peers) que tiene como objetivo el uso compartido de recursos distribuidos en un entorno de red evitando los servicios centrales” (Oram, 2001).

Una red peer-to-peer, red de pares, red entre iguales o red entre pares (P2P, por sus siglas en inglés) es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino como una serie de nodos que se comportan como iguales entre sí, donde "los usuarios que participan pueden establecer una red virtual, totalmente independiente de la red física, sin tener que obedecer a cualquier autoridad administrativa o restricciones" (Steinmetz & Wehrle, 2005).

Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados. Normalmente este tipo de redes se implementan como redes superpuestas construidas en la capa de aplicación de redes públicas como Internet. El hecho de que sirvan para compartir e intercambiar información de forma directa entre dos o más usuarios ha propiciado que parte de los usuarios lo utilicen para intercambiar archivos cuyo contenido está sujeto a las leyes de copyright, lo que ha generado una gran polémica entre defensores y detractores de estos sistemas. Las redes peer-to-peer aprovechan, administran y optimizan el uso del ancho de banda de los demás usuarios de la red por medio de la conectividad entre los mismos, y obtienen así más rendimiento en las conexiones y transferencias que con algunos métodos centralizados convencionales, donde una cantidad relativamente pequeña de servidores provee el total del ancho de banda y recursos compartidos para un servicio o aplicación. (Wikipedia, 2019). Cuando las redes Peer-to-Peer usan algún tipo de mecanismo de consenso se las denomina **Redes Crypto**.

Funciones Resumen o HASH

A las funciones resumen, también se les llama funciones hash o funciones digest. Una función hash es una función computable, mediante un algoritmo tal que tiene como entrada un conjunto de elementos, que suelen ser cadenas de longitud variable, y los convierte en un rango de salida finito, normalmente cadenas de longitud fija. Es decir, la función actúa como una proyección del conjunto entrada sobre el conjunto salida. La idea básica de un valor *hash* es que sirva como una representación compacta de la cadena de entrada. (Wikipedia, 2020)

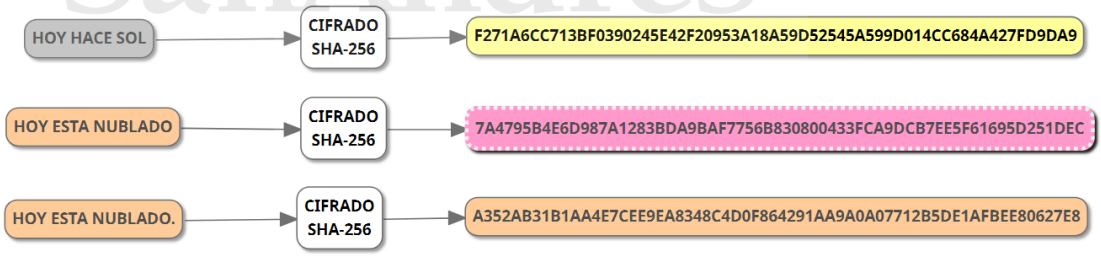


Ilustración 6 - Ejemplos de hash (Bit2me Academy)

Una función hash criptográfica; es una función hash que es adecuada para su uso en criptografía. Es un algoritmo matemático que asigna datos de tamaño arbitrario (a menudo llamado "mensaje") a una cadena de bits de un tamaño fijo (el "valor hash", "hash" o "resumen de mensaje") y es función unidireccional, es decir, una función que es prácticamente imposible de invertir. Idealmente, la única forma de encontrar un mensaje que produzca un hash dado es intentar una búsqueda de fuerza bruta de posibles entradas para ver si producen una coincidencia, o usar una tabla de hashes coincidentes. Las funciones hash criptográficas son una herramienta básica de la criptografía moderna.

La función hash criptográfica ideal tiene las siguientes propiedades principales:

- Es determinista, lo que significa que el mismo mensaje siempre da como resultado el mismo hash.
- Es rápido calcular el valor hash para cualquier mensaje dado.
- No es factible generar un mensaje que produzca un valor hash dado.
- No es factible encontrar dos mensajes diferentes con el mismo valor hash.
- Un pequeño cambio en un mensaje debería cambiar el valor de hash de manera tan extensa que el nuevo valor de hash parece no estar relacionado con el valor de hash anterior (efecto de avalancha). (Wikipedia, 2020)

Árbol de Merkle

Un árbol hash de Merkle (en inglés Merkle Hash Tree) o árbol de merkle o árbol hash es una estructura de datos en árbol, binario o no, en el que cada nodo que no es una hoja, está etiquetado con el hash de la concatenación de las etiquetas o valores (para nodos hoja) de sus nodos hijo. Son una generalización de las listas hash y las cadenas hash.

Permite que gran número de datos separados puedan ser ligados a un único valor de hash, el hash del nodo raíz del árbol. De esta forma proporciona un método de verificación segura y eficiente de los contenidos de grandes estructuras de datos. En sus aplicaciones prácticas normalmente el hash del nodo raíz va firmado para asegurar su integridad y que la verificación sea totalmente fiable. La demostración de que un nodo hoja es parte de un árbol hash dado requiere una cantidad de datos proporcional al logaritmo del número de nodos del árbol. Fue patentado en 1979 por Ralph Merkle. (Wikipedia, 2020)

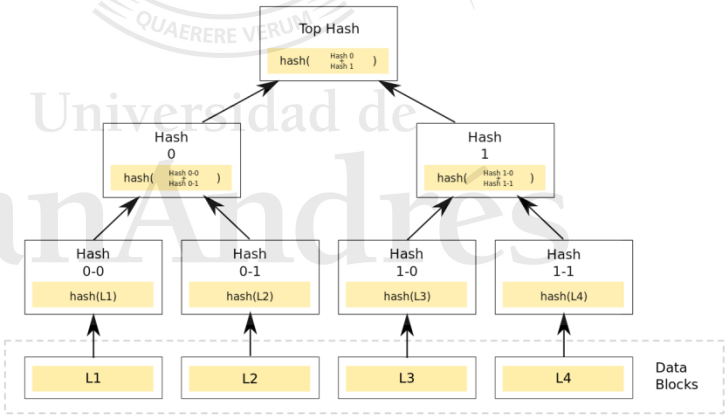


Ilustración 7 - Merkel Tree (Original illustration by David Göthberg, Sweden)

Criptografía asimétrica

La criptografía asimétrica o infraestructura de clave pública, es una de las técnicas más usadas en informática y parte fundamental de la seguridad de redes como Internet y las blockchain/DLT; consistente en la utilización de una fórmula matemática compleja para generar un par de claves: una clave privada que es de uso y conocimiento exclusivo del creador y una clave pública que se comparte con terceras personas.

Con la clave privada se crea fácilmente una clave pública; pero el proceso reverso, es prácticamente intratable computacionalmente. El creador de las claves (se generan juntas), puede distribuir la clave

pública con terceras personas, para que éstas le puedan enviar mensajes cifrados con esa clave de modo que solo él la pueda descifrar mediante el uso de la clave su privada.

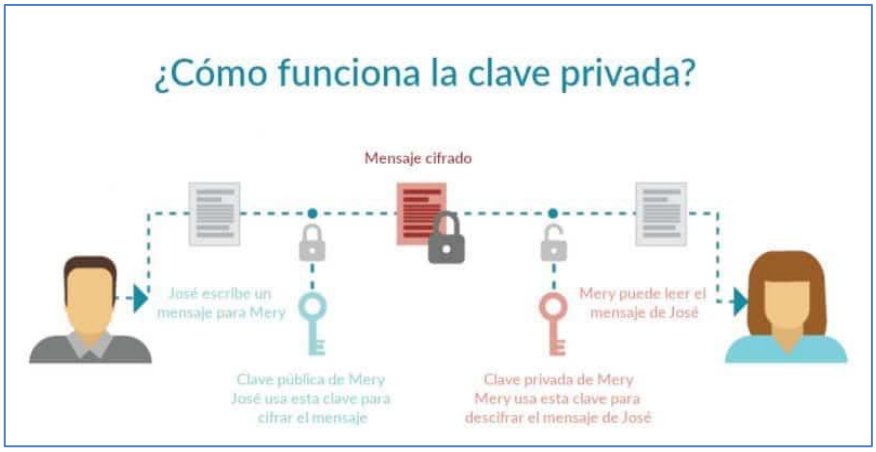


Ilustración 8 - Como funciona PKI (Bit2me Academy, 2020)

La infraestructura de cifrado asimétrico fue inventada por Merkle, Diffie y Hellman (MDH) en 1976, garantizando con este esquema comunicaciones completamente seguras sobre canales inseguros; siendo en la actualidad el método de cifrado más usado en Internet.

Cuando se decide el uso del sistema de criptografía pública se debe en principio definir qué algoritmo de cifrado asimétrico se usará (ej., SHA256, Curve25519, secp256k1, etc.). Seguidamente se procede a la generación de la clave privada usando un generador de números aleatorios muy seguro y una pool de entropía[8], para obtener un número aleatorio, que aplicado a una función matemática genera un número aleatorio suficientemente grande, como para garantizar la seguridad de la clave. Este número se aplica como entrada a la función criptográfica y se logra una cadena de caracteres que es la "clave privada". Con la clave privada, se genera la clave pública que se utiliza para cifrar mensajes que se pueden descifrar con nuestra clave privada.

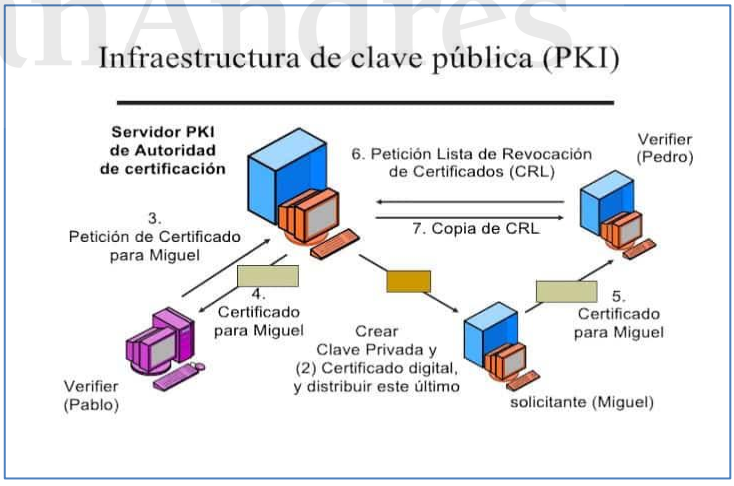


Ilustración 9 - Infraestructura de clave asimétrica (Bit2me Academy, 2020)

Para el funcionamiento de un sistema de cifrado es necesaria la propagación segura de las claves; para esto se pueden optar por los siguientes métodos (o combinación de ellos):

[8] Un "pool de entropía" es una fuente de aleatoriedad necesaria para operaciones como el cifrado. Puede estar implementado en hardware, software o fusión de ambos. Aprovecha circunstancias aleatorias del sistema (real del hardware, movimientos del mouse, pulsación de teclas, etc.) para generar números aleatorios.

- Infraestructura de clave pública o PKI. En la infraestructura PKI existen una o varias entidades emisoras de certificados. Cada entidad posee un nivel de confianza, que sirve para certificar la autenticidad de las claves públicas. Se usa principalmente en Internet para asegurar la autenticidad de los certificados SSL/TLS de las páginas webs.
- Red de confianza. Cada usuario establece una serie de corresponsales con los que comparte su clave pública de forma abierta o privada. Este esquema de propagación es utilizado en sistemas como PGP en el envío de correos privados y cifrados.
- Criptografía basada en identidad real o virtual. Este sistema de propagación utiliza un sistema centralizado que gestiona nuestras claves, las cuales están relacionadas con la identidad real o virtual que se proporcionó al sistema.
- Criptografía basada en certificados. El usuario debe poseer un conjunto de clave pública/privada. La clave es remitida a una autoridad de certificación, para que utilizando criptografía basada en identidad, genere un certificado que asegure la validez de los datos.
- Criptografía sin certificados. Este modelo es parecido al anterior con la salvedad que la clave privada generada por la autoridad es parcial. La clave privada final depende de la clave privada parcial y un número aleatorio calculado por el usuario. Esto garantiza un mayor nivel de seguridad.

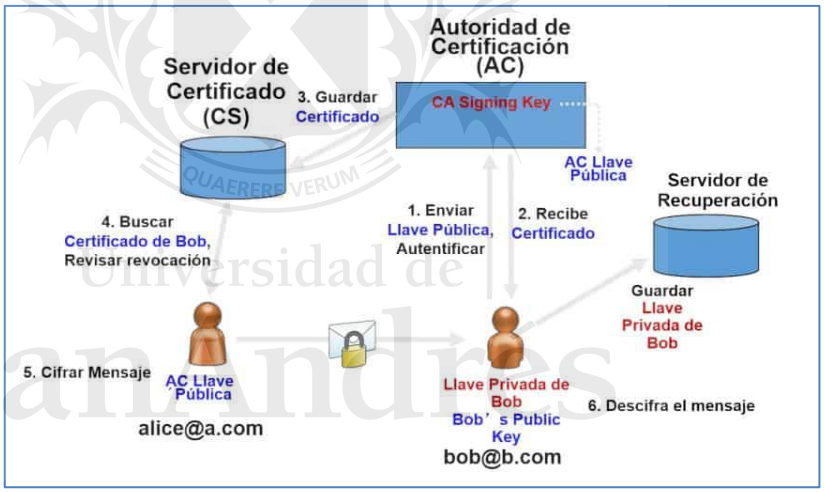


Ilustración 10 - Autoridad de Certificación (Bit2me Academy, 2020)

Después de propagadas las claves públicas de forma segura (protocolo SSH[9]), podemos empezar a utilizar el sistema para enviar y recibir mensajes de forma segura. Este esquema de envío y recepción funciona generalmente de la siguiente forma:

1. Bob genera un mensaje el cual es cifrado usando la clave pública de Alice, y firmado con la clave privada de Bob. Esto garantiza que el mensaje solo pueda ser visto por Alice y ella puede corroborar que inequívocamente proviene de Juan.

[9] SSH (o Secure SHell) es un protocolo cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada. SSH permite copiar datos de forma segura (tanto archivos sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir contraseñas al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH. (Bit2me Academy, 2020)

2. El mensaje viaja firmado y cifrado por el canal de comunicación. Si es interceptado el esfuerzo será fútil porque no se podrá leer información alguna del mismo.
3. Una vez que el mensaje llega a su destinatario Alice, ella usará su clave privada para descifrarlo. Al mismo tiempo, podrá usar la clave pública de Juan para validar que realmente el mensaje ha sido enviado por él.

QUAERERE VERUM
Universidad de
SanAndrés

Principales blockchain/DLTs

En este capítulo veremos los principales blockchain que existen y en un capitulo posteriormente veremos en conjunto las ventajas y desventajas de cada uno comparativamente.

Bitcoin

En el año 2009, Satoshi Nakamoto[10] publicó un white paper denominado "Bitcoin: Un sistema de efectivo electrónico usuario-a-usuario". En él se destaca que "una forma de dinero en efectivo electrónico puramente peer-to-peer debería permitir enviar pagos online directamente entre las partes y sin pasar a través de una institución financiera. Las firmas digitales son parte de la solución, pero los beneficios principales desaparecen si un tercero de confianza sigue siendo imprescindible para prevenir el doble gasto. Proponemos una solución para el problema del doble gasto usando una red peer-to-peer. La red sella las transacciones en el tiempo en una cadena continua de proof-of-work basada en hash, estableciendo un registro que no se puede modificar sin rehacer la proof-of-work. La cadena más larga no solo sirve de prueba efectiva de la secuencia de eventos, sino que también demuestra que procede del conjunto de CPU más potente. Mientras la mayoría de la potencia CPU esté controlada por nodos que no cooperen para atacar la propia red, se generará la cadena más larga y se aventajará a los atacantes. La red en sí misma precisa de una estructura mínima. Los mensajes se transmiten en base a 'mejor esfuerzo', y los nodos pueden abandonar la red y regresar a ella a voluntad, aceptando la cadena proof-of-work más larga como prueba de lo que ha sucedido durante su ausencia". (Nakamoto, 2009).

Según (Pérez, 2016) Nakamoto después de dos años de desarrollo del proyecto transfirió los dominios de Bitcoin a la comunidad Bitcoin y abandonó el proyecto para siempre. El repositorio del código fuente y la clave de alerta de red fue transferida en principio a Gavin Andresen, quién en 2014 dejó esta responsabilidad en manos del holandés Wladimir van der Laan. Se desconoce la verdadera identidad de Nakamoto; se cree por la calidad del trabajo que ni siquiera se trata de una sola persona, sino más bien de un grupo de científicos y programadores (Wallece, 2011). Sus méritos llevaron a que el profesor PhD de finanzas Bhagwan Chowdhry (UCLA) lo propusiera para el Premio Nobel de Economía en 2016 (Chowdhry, 2015), aunque la academia sueca no aceptó su nominación por tratarse de una persona anónima.

Usuarios

En Bitcoin los usuarios meramente transaccionales pueden realizar sus transacciones y manejar sus identidades digitales mediante billeteras digitales, que son las interfaces gráficas con que se interactúa con la red. Hay otros usuarios denominados mineros, que intentan resolver el acertijo matemático que se propone y que resulta necesario para poder tener el derecho para adicionar el próximo bloque a la cadena de transacciones. Estos usuarios son recompensados por su tarea con un pago en la propia moneda digital que se crea a tal efectos y también puede recibir un pago (fee) de parte de los usuarios que desean sus transacciones tengan preferencia para ser incorporadas al bloque. El monto que el

[10] Satoshi Nakamoto es la persona o grupo de personas que crearon el protocolo Bitcoin y su software de referencia. En 2008, Nakamoto publicó un artículo en la lista de correo de criptografía metzdowd.com que describía un sistema P2P de dinero digital. En 2009, lanzó el software Bitcoin, creando la red del mismo nombre y las primeras unidades de moneda, llamadas bitcoins. La verdadera identidad de Nakamoto sigue siendo desconocida y ha sido objeto de mucha especulación. No se sabe si el nombre «Satoshi Nakamoto» es real o un seudónimo, o si el nombre representa a una persona o grupo de personas. (Wikipedia, 2020)

sistema genera como recompensa para el minero, es el único modo en que se puede crear nueva moneda en la red, y esto evita que se genere inflación; porque está perfectamente determinado la cantidad de bitcoins que se crearán.

Como se trata de una red peer to peer, cada usuario es un nodo de la red; y almacena en su dispositivo una copia exacta y completa del libro contable. Los nodos mineros, reciben todas las transacciones que se hacen en la red y las agrupa para proponerlas como trabajo a los mineros. El acertijo consiste en encontrar un "nonce"[11] , y cuando un nodo minero logra resolverlo, distribuye en la red el nuevo bloque propuesto y el valor del nonce para su validación. Se necesita la confirmación de una determinada cantidad de bloques para que éste se añada a la cadena haciendo referencia al bloque anterior; y de esta manera se van "encadenando" consecutivamente. En el bloque propuesto, como primera transacción se incluye el valor la recompensa, que es el monto de emisión de moneda que hace la red y que se adjudican a la cartera del minero ganador.

El bloque

La cadena de bloque comienza con una génesis o bloque inicial; a partir de este bloque, todo nuevo bloque dependerá del bloque anterior, así que el primer bloque hace referencia al génesis o inicial.

Cada bloque tiene los siguientes elementos:

- Índice: indica el número de orden del bloque en la cadena.
- Hash: El hash es calculado usando el algoritmo criptográfico utilizado SHA256, tomando como entradas: el índice, el hash previo, la marca de tiempo, las transacciones y un nonce.
- Hash Previo: Es el hash del bloque previo.
- Marca de tiempo (time stamp): Indica cuando fue creado el bloque y contiene una marca de tiempo de Unix [12]. La marca de tiempo es válida si es mayor que la mediana de los 11 bloques previos, y menor que el tiempo ajustado por la red + 2 horas. A su vez, el "tiempo ajustado por la red" es la mediana de las marcas de tiempo devueltas por todos los nodos conectados al propio nodo. Las marcas de tiempo de bloque no son precisamente exactas y no necesitan estar en orden.
- Datos: Son las transacciones que se almacenan en el bloque. Veremos con mayor detalle la transacción más adelante.
- Nonce: El "nonce" de un bloque bitcoin es un campo de 32 bits (4 bytes) que representa el número de iteraciones se hicieron hasta que se resolvió correctamente el bloque. Su valor se establece de modo que el hash del bloque contenga una ristra de ceros. Como el resto de los campos de la transacción no se pueden variar ya que tienen un significado definido. Se utiliza el nonce como variable para que el hash del bloque sea completamente diferente, dado que es imposible predecir qué combinación de bits se traducirá en el hash correcto. Se intentan muchos nonce diferentes y el hash se vuelve a calcular para cada valor hasta que se encuentre un hash que contenga el número necesario de bits a cero al comienzo. Como este cálculo

[11] El "nonce" de un bloque bitcoin es un campo de 32 bits (4 bytes) que se verá más adelante.

[12] Una marca de tiempo de Unix. El tiempo Unix (POSIX) es un sistema para describir un punto en el tiempo . Es el número de segundos que han transcurrido desde las 00:00:00 del jueves 1 de enero de 1970 (UTC), menos los segundos del salto. Cada día se trata como si contuviera exactamente 86 400 segundos, por lo que los segundos de salto se deben restar desde la época.

iterativo requiere tiempo y recursos, el cálculo del valor del nonce correcto es la prueba de trabajo.

Los nodos mineros comienzan a escanear el valor del nonce, de modo tal que al ser incorporado como entrada a la función hash, el resultante comienza con la cantidad requerida de ceros. Este proceso iterativo de probar diversos valores al azar hasta encontrar el correcto se llama minería. El minero que encuentra el valor del nonce, agrega a el nuevo bloque a su red local y luego a través de la red peer to peer, se transmite al resto de los nodos de la red, quienes pueden fácilmente validar el hash y confirmar el bloque.

El nivel de dificultad se ajusta de manera dinámica para garantizar la creación de un nuevo bloque en un promedio de diez minutos. El control del flujo se regula mediante el grado de dificultad para obtener el nonce. Si en promedio la capacidad de cálculo aumenta, el tiempo promedio disminuye, entonces para compensar se debe aumentar la dificultad para hallar el nonce. Si la capacidad de cálculo baja, el tiempo promedio aumentaría, entonces se disminuye la dificultad para obtener el nonce y así disminuir el tiempo promedio. Esta dificultad se regula, requiriendo mayor o menor cantidad de ceros al inicio del hash. A mayor cantidad de ceros, mayor dificultad.

Una vez que el minero ha realizado la prueba de trabajo, se agrega el nuevo bloque a la red local del minero ganador y se transmite al resto de la red informando el nonce que resuelve el hash; por lo que resulta fácilmente confirmar la validez del hash.

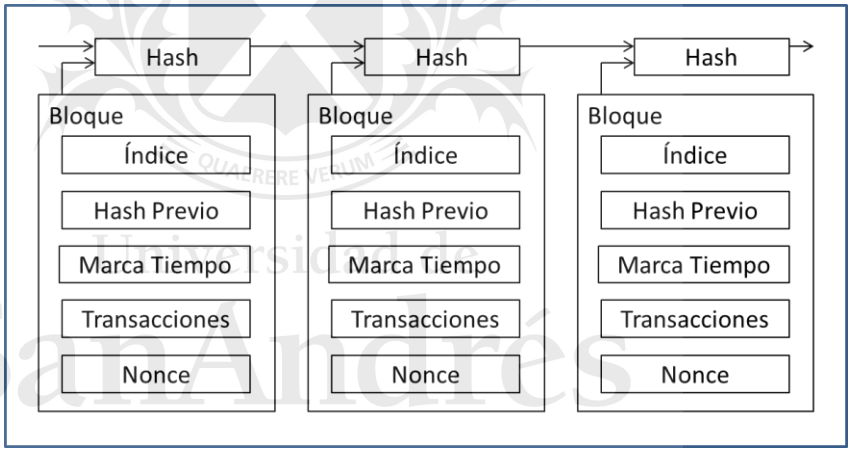


Ilustración 11 - Esquema de transacciones de Bitcoin (elaboración propia)

La inmutabilidad del blockchain se garantiza, en razón que para cambiar el bloque, se debería rehacer todo el trabajo de minería; y como cada diez minutos se van agregando nuevos bloques que incorporan el hash del anterior, también se deberían cambiar los sucesivos bloques, por lo que es casi imposible para alterar la cadena.

Para poder hacer transferencias, es necesario contar con una billetera electrónica, donde se firma digitalmente la transacción para garantizar la seguridad del envío del activo. En esta billetera se pueden acumular activos o para realizar transacciones de compra de bienes y servicios y está asociada a una dirección de bitcoin.

La billetera electrónica es en realidad un programa necesario para enviar y recibir criptoactivos, que contiene las llaves criptográficas (claves privadas, únicas, irrepetibles y secretas) con las que se garantiza el saldo y titularidad de los criptoactivos que contiene. Es el equivalente a una cuenta bancaria, pues consiste en un número que indica la dirección desde la que se realizan o reciben las transferencias. Esta dirección es un identificador de entre 27 y 34 caracteres alfanuméricos,

comenzando por el número 1 o el 3, que representa un destino de un pago, de bitcoins u otro criptoactivo. Las direcciones se generar de forma automática por la billetera.

La dirección en particular no contiene los activos digitales guardados en ella, solo guarda el registro de las transacciones entre las diferentes direcciones y la variación de los saldos. Todas las transacciones se almacenan luego en el gran libro de contabilidad pública que es el blockchain.

Cuando vamos hacer una transferencia, tenemos que tener en cuenta tres aspectos:

- El input o entrada, que nos indica el saldo que se posee en la billetera.
- La cantidad que se desea transferir.
- Un output o salida, que indica la dirección de la billetera que va recibir la transacción.

Para enviar un determinado monto se necesitan la dirección BTC[13] de destinatario y la clave privada del usuario que hace el envío para para confirmar la transacción.

Es recomendable que se utilice una dirección diferente para cada transacción en la que se reciban activos digitales, para evitar que se asocien las direcciones con la persona que recibe los envíos y se sepan la cantidad de Bitcoin que se han recibidos.

Una vez realizada la transferencia, los mineros BTC verifican la transacción y la ubican junto a otras transacciones en un bloque, el que proponen como candidato para ser validado e incorporado a la cadena.

Para que se complete un bloque, se deben verificar e incorporar muchas transacciones. El protocolo Bitcoin está concebido de manera que se agregue un bloque aproximadamente cada diez minutos en promedio y dispone de mecanismos de regulación para ajustar ese ritmo.

Para asegurarse que su transacción sea incorporada lo más rápido posible, se pueden añadir como parte de la transacción una comisión para el minero de modo que la transferencia resulte más atractiva para los mineros y de esta forma que se procese mucho más rápido a través de la red.

Una transacción está compuesta por entradas (inputs) y salidas (outputs). Las salidas se denominan “transacciones no gastadas” o UTXO (unspent transaction outputs). Las entradas contienen UTXOs de una transacción anterior y una “secuencia de comandos de desbloqueo” por cada uno de los UTXO de entrada.

La cadena de blockchain tiene un historial de todas las transacciones hechas por cada usuario, es decir el registro de todas las UTXO de transacciones realizadas por el usuario. Para que la billetera electrónica refleje el saldo del usuario debe buscar en toda la cadena de bloques los UTXO que controla la clave privada de ese usuario y sumar los valores de los UTXO, para poder obtener el saldo actual.

La UTXO es una unidad de valor discreta e indivisible denominada Satoshi. Cada Satoshi vale la cien millonésima avas partes de un Bitcoin (1 / 100.000.000 Bitcoins) y es su fracción más pequeña. Los UTXOs previenen los ataques de doble gasto y evitan el gasto de monedas inexistentes. La red mantienen una base de datos que contiene todos los UTXOs disponibles para gastar, por eso los nodos rechazarán cualquier transacción que invoque UTXOs que no están en esa base de datos.

Para permitir la división y combinaciones de valores, las transacciones pueden contener múltiples entradas y salidas. Podrá ser una entrada simple de una transacción anterior mayor, o múltiples entradas combinando pequeñas cantidades. Como máximo tienen dos salidas: una para el pago a la

[13] BTC = Bitcoin

dirección de destinatario y otra con el cambio dirigida al emisor. Cuando el valor a gastar es menor a la UTXO, se genera un pago por el valor de la transacción a la dirección del destinatario y el resto se envía a la dirección del promotor. Algunas billeteras electrónicas por razones de seguridad y anonimato, dividen ese resto o "vuelto" en varias direcciones de la cuenta del emisor generadas aleatoriamente para dificultar la trazabilidad de esos fondos.

Las transacciones denominadas "coinbase" son las primeras transacciones de cada bloque y tienen la particularidad que no consumen UTXOs generados por una instancia anterior, sino que se generan a partir de las comisiones de las transacciones que en ese bloque se pagarán al minero que minó el bloque.

El valor de las comisiones por transacción (fees) es la diferencia entre la entrada total y la salida total; y no hay en la estructura de la transacción ningún campo destinado a guardar la tarifa. Los mineros conocen la tarifa que conlleva la transacción, calculando la diferencia que existe entre la suma de todos los valores de entrada de la transacción y la suma de todos los valores de salida. Por eso se debe prever una salida menor a la entrada para que los mineros se interesen en incorporar la transacción al bloque, porque si bien las tarifas no son obligatorias, las transacciones con tarifa cero pueden no ser minadas ni propagarse por la red.

Nuevo UTXO = (∑ UTXO entrada) – [(∑ UTXO salida) - (Tarifa)]

Las tarifas además de compensar a los mineros, actúan como una protección de la red (anti spam), porque al tener un costo (económico y temporal) disuaden a que se envíen transacciones en forma constante.

Para determinar el monto de la comisión, se analiza la complejidad de la transacción a partir de su tamaño en kilobytes y no por la cantidad de bitcoins que se están transaccionando. Esto puede derivar en que el envío de un pequeño monto en una transacción compleja, cueste más que enviar una gran suma en una transacción sencilla. Los cálculos de la comisión se pueden hacer dinámicamente y el emisor puede optar por tarifas altas, medias o bajas, según su prisa e interés en el procesamiento de la transacción. También, algunas billeteras incorporan en su software algoritmos que estiman la cuota más baja posible a pagar para que esta sea aceptada.

Las UTXOs solo pueden ser "gastadas" mediante transacciones, es decir ser "entradas" de nuevas transacciones y las "entradas" están compuestas por pares de UTXOs y "secuencias de comando de desbloque", es decir que a cada transacción le corresponde una secuencia de desbloqueo.

Las UTXOs de salida indican la dirección de la billetera que va recibir la transacción y se propagan en la red por lo que son visibles por todos los nodos. Para validar que la transacción sólo pueda ser gastada por el propietario (dirección del destinatario), en cada transacción se pone a la salida un script de "bloqueo" que especifica la condición que debe cumplir la "secuencia de comandos de desbloqueo" para que la transacción pueda ser gastada. Los nodos que validan las transacciones ejecutando los scripts de bloqueo y desbloqueo, y si el script de desbloqueo cumple las condiciones del script de bloqueo, la transacción se considera válida.

Los scripts de bloqueo y desbloqueo se programan en un lenguaje "turing incompleto" llamado "script", que posee una complejidad limitada ya que carece de la capacidad de controlar bucles o flujos complejos, como "while" o "loops". Esta característica si bien reduce las posibilidades de programación, mejora los tiempos de ejecución y lo hace menos propenso a errores de programación del que puedan valerse los hackers para modificar su comportamiento. Sin embargo, la lógica que se

puede introducir en los scripts, puede ser lo suficientemente compleja como el programador desee, de modo que las condiciones pueden contener una gran variedad de condiciones que se deban cumplir.

En general las transacciones en la red de bitcoin se bloquean con un script de "pago a clave pública" (P2PKH – pay to public key) por lo que solo se puede gastar procesando el script de desbloqueo de la UTXO y proporcionando la clave pública y la firma digital creada por la clave privada correspondiente. Si la transacción se valida, se agrega a un bloque para propagarse en la red.

Los nodos almacenan la base de datos UTXO en la RAM o pueden optar por almacenar parte de ella en un disco de estado sólido (SSD) o en un disco duro mecánico. Los tiempos de validación deberán mantenerse por debajo del tiempo promedio de bloque de diez minutos.

Ethereum

Ethereum es una cadena de bloques pública, de código abierto y una plataforma de computación descentralizada que ofrece una completa funcionalidad de contrato inteligente. Propuesto a finales de 2013, por Vitalik Buterin[14], como una plataforma que podría aprovechar el blockchain para almacenar y ejecutar programas informáticos en una red internacional de nodos distribuidos. Ethereum se ha convertido en la plataforma más conocida y utilizada después de Bitcoin. (Curran, 2019)

"Lo que Ethereum pretende proporcionar es una cadena de bloques con un lenguaje de programación Turing completo integrado en el que se puede usar para crear 'contratos ' que se pueden usar para codificar funciones de transición de estado arbitrarias, permitiendo a los usuarios crear cualquiera de los sistemas descritos arriba, así como muchos otros que aún no hemos imaginado, simplemente escribiendo la lógica en unas pocas líneas de código" (Vitalik Buterin, 2014)

Las aplicaciones construidas en la parte superior de la cadena de bloques de Ethereum se denominan Daap, y son aplicaciones descentralizadas, es decir, una App que no depende de un sistema central, sino que depende de la comunidad de usuarios que la utilizan. La aplicación descentralizada puede ser una app móvil o una aplicación web que interactúa con un contrato inteligente para llevar a cabo su función.

Los contratos inteligentes son la característica principal de Ethereum y básicamente son programas autoejecutables que facilitan el intercambio de cualquier cosa de valor en la red, almacenada de forma inmutable en la cadena de bloques. Se ejecutan cuando se cumplen condiciones específicas y están fuera de la influencia de terceros o la censura y no tienen tiempo de inactividad, siempre y cuando la red Ethereum esté funcionando.

La innovación central de la plataforma fue la "Máquina Virtual de Ethereum" (EVM) y es un software turing completo que se ejecuta en la red de Ethereum, lo que permite ejecutar cualquier programa, en la cadena de bloques de Ethereum, independientemente del lenguaje de programación; con la posibilidad de crear una amplia gama de aplicaciones descentralizadas, todo en una sola plataforma.

El desarrollo de Ethereum se inició a través de la compañía suiza Ethereum Switzerland GmbH y, posteriormente, a través de la Fundación sin fines de lucro Ethereum. En julio de 2014, Ethereum se sometió a una venta masiva donde se recaudaron más de $ 14 millones entre julio y agosto. En septiembre del mismo año, el Éter (la moneda Ethereum) se distribuyó a los inversores y al equipo de desarrollo, mientras que los fondos restantes se destinaron a la Fundación Ethereum.

[14] Vitalik Buterin es un programador y escritor ruso, cofundador de Ethereum y de Bitcoin Magazine.

En julio de 2015, se lanzó la primera versión principal, lanzamiento experimental de Ethereum que se denominó "Frontier". La primera actualización importante a la plataforma Ethereum se lanzó en marzo de 2016 como "Homestead" y fue la primera actualización que se consideró estable, centrándose en los precios del gas, la seguridad y el procesamiento de transacciones.

Una Organización Autónoma Descentralizada (DAO) funciona como un fondo de capital de riesgo dirigido por inversionistas. Una DAO plenamente funcional, cuenta con un conjunto de reglas pre-programadas, funciona de forma autónoma y se coordina a través de un protocolo de consenso distribuido. Esas reglas están codificadas como un contrato inteligente, que es esencialmente un programa de computadora, que existe autónomamente en Internet, pero al mismo tiempo necesita que la gente realice tareas que no puede hacer por sí mismo. Una vez establecidas las reglas, la DAO entra en una fase de financiación, porque debe tener algún tipo de recursos (tokens) que pueden ser gastados por la organización o utilizados para recompensar ciertas actividades dentro de ella. Los usuarios que invierten en la DAO, obtienen derechos de voto y, posteriormente, la posibilidad de influir en su funcionamiento.

Desafortunadamente la DAO Slack, fue pirateada en junio de 2016, cuando usuarios desconocidos pudieron explotar una vulnerabilidad en su código y pudieron transferir $ 50 millones a un DAO diferente (conocido como Dark DAO). Además, una vez públicos, otros usuarios utilizaron la misma vulnerabilidad para desviar los fondos restantes a un tercer DAO llamado el DAO de White Hat. (Jentzsch, 2016)

En julio de 2016, Vitalik Buterin anunció que los mineros habían acordado la bifurcación dura de la cadena. Sin embargo, una minoría de los mineros se mantuvo firme en sus convicciones de no cumplir con el protocolo. Por lo tanto, Ethereum se bifurcó y la nueva cadena se conoció como Ethereum y la cadena antigua se conoció como Ethereum Classic, dividiendo a la comunidad Ethereum. A medida que avanzaba el tiempo, la mayoría de las empresas, desarrolladores, mineros y usuarios favorecieron la cadena Ethereum (bifurcada) y es la cadena actual denominada Ethereum con la segunda capitalización de mercado más alta y una vasta comunidad detrás. Sin embargo, Ethereum Classic (ETC) también sigue siendo una criptomoneda popular, ya que el equipo detrás de ETC implementa las mismas actualizaciones que la cadena Ethereum y también desarrolla activamente la plataforma.

La máquina virtual Ethereum (EVM) es un software Turing completo que se ejecuta en la red de Ethereum. Corre scripts en una red distribuida y permite la ejecución y almacenamiento de todo, desde contratos inteligentes hasta DAO. Funcionalmente, Ethereum permite a los desarrolladores crear aplicaciones descentralizadas, incluyendo juegos, registros distribuidos, organizaciones y muchos más.

El diseño detrás de Ethereum, pretende seguir los principios de:

- Simplicidad: el protocolo debe ser lo más eficiente posible, incluso a costa del almacenamiento de datos o de las ineficiencias de tiempo.
- Universalidad: un script interno de Turing-completo se proporciona en un lenguaje que un desarrollador puede usar para programar cualquier contrato inteligente o tipo de transacción.
- Modularidad: el protocolo Ethereum debe diseñarse para que sea lo más modular y separable posible.
- Agilidad: el protocolo no está establecido en piedra y se aprovechará cualquier oportunidad para mejorar la arquitectura del protocolo o el EVM en escalabilidad o seguridad.
- No discriminación / No censura: el protocolo no debe intentar restringir o prevenir activamente categorías específicas de uso. (Chinchilla, 2019)

Los beneficios de Ethereum no solo como una plataforma basada en blockchain, sino también en comparación con otras plataformas basadas en blockchain incluyen:

- Inmutabilidad: un tercero no puede realizar ningún cambio en los datos.
- Prueba de corrupción / manipulación: la censura no es factible con el consenso de PoW de la red vasta y descentralizada que está de acuerdo con su estado global.
- Seguridad: la combinación del consenso de PoW, las técnicas criptográficas utilizadas en el modelo de transacción y la falta de un punto central de falla protegen la red contra la piratería y la manipulación.
- Sin tiempo de inactividad: las aplicaciones, los contratos inteligentes, las organizaciones, etc., que se ejecutan en la cadena de bloques Ethereum siempre se están ejecutando y no se pueden desactivar.

Como plataforma completa de turing, Ethereum es susceptible a las vulnerabilidades que pueden ser explotadas a través de la complejidad del lenguaje de programación primario utilizado en los contratos inteligentes, Solidity. La seguridad de los contratos inteligentes se ha convertido en una de las principales preocupaciones y el hackeo de la DAO fue un evento que marcó a la comunidad de usuarios y dejó gran preocupación sobre la viabilidad de los contratos inteligentes a largo plazo. La enseñanza que dejó ese incidente, es que se deben extremar los controles antes de lanzar una Dapp. Subsidiariamente se establecieron algunas recomendaciones para evitar que incidentes como el descripto, causen mayores daños.

Ethereum privilegia la seguridad y la descentralización por sobre la escalabilidad; comprometiendo su rendimiento e incrementando los costos de gas; lo que genera una desventaja para los usuarios, que en general buscan un uso gratuito de aplicaciones. Ethereum no utiliza el modelo de saldos de UTXO; sino un sistema de cuentas que consisten en direcciones de 20 bytes y donde cada transacción de valor o información se considera una transición de estado. Una cuenta de Ethereum contiene 4 campos. El nonce, el saldo de éter, el código del contrato y el del almacenamiento. Existen dos tipos de cuentas; externas y de contrato. Las externas son cuentas de usuario controladas por claves privadas, no contienen código y se usan para crear y firmar transacciones. Las cuentas de contrato son un contrato inteligente, ejecutado por código y que recibe mensajes que permiten almacenar mensajes y código, así como interactuar con otros contratos o cuentas externas.

Éter es la moneda de la plataforma Ethereum, mientras que el “gas” es el éter que se utiliza para pagar transacciones y cálculos en la red. Ethereum no almacena la lista de transacciones, sino el estado más reciente de la red.

Ethereum emplea un modelo de consenso de prueba de trabajo (PoW) modificado; que es extremadamente seguro, ya que la red consta de miles de nodos descentralizados en todo el mundo. El modelo de consenso utiliza el algoritmo Ethash (DAG)[15], diseñado para una verificación rápida.

Los contratos inteligentes y la posibilidad que se puedan desarrollar aplicaciones descentralizadas (dapps) es una de las características más destacadas de Ethereum. Solidity es el lenguaje de programación más utilizado, sin embargo existes la posibilidad de utilizar otros lenguajes como Go, C++ y Python.

[15] DAG (gráfico acíclico dirigido) es un conjunto de datos grande, transitorio y generado aleatoriamente para el algoritmo de prueba de trabajo (https://github.com/ethereum/wiki/wiki/Mining#the-algorithm)

En conclusión; Ethereum es una de las plataformas más importantes y populares en la industria de blockchain y su adopción se generaliza, en la medida que se implementan cada vez más contratos inteligentes.

Quórum

Quorum es un protocolo de libro mayor distribuido basado en Ethereum que se ha desarrollado para proporcionar a la industria de servicios financieros sobre una implementación autorizada de Ethereum que respalde la privacidad de las transacciones y los contratos. (jpmorganchase/cuorum, 2018)

El protocolo Quórum incluye una bifurcación minimalista del cliente de Go Ethereum[16], que está disponible como un cliente independiente llamado Geth que se puede instalar en casi cualquier sistema operativo, o como una biblioteca que se puede incrustar en proyectos Go, Android o iOS. De esta forma se aprovecha el trabajo de actualizaciones que la comunidad que desarrolladores de Ethereum han emprendido.

Las características principales de Quorum, y por lo tanto las extensiones sobre Ethereum público, son:

- Transacciones y privacidad del contrato.
- Múltiples mecanismos de consenso basados en la votación.
- Gestión de permisos de red / pares
- Mayor rendimiento / escalabilidad

Si bien Quorum se diseñó teniendo en cuenta los casos de uso de los servicios financieros, su implementación no es específica de los servicios financieros exclusivamente y, por lo tanto, es adecuada para otras industrias que estén interesadas en utilizar Ethereum, pero que requieran las características mencionadas anteriormente.

El nodo de Quórum está diseñado intencionalmente para ser una bifurcación liviana de “Geth”[17] para que pueda continuar aprovechando la I+D que se está llevando a cabo dentro de la comunidad Ethereum, en constante crecimiento. Para ese fin, Quorum se actualizará en línea con las futuras versiones de geth.

El nodo de Quórum incluye las siguientes modificaciones para geth:

- Se logra el consenso con los algoritmos de consenso BFT de Raft o Estambul en lugar de usar la Prueba de Trabajo (PoW).
- La capa P2P se ha modificado para permitir solo conexiones a/desde nodos autorizados.
- La lógica de generación de bloques se ha modificado para reemplazar la comprobación de "raíz de estado global" con una nueva "raíz de estado público global".
- La lógica de validación del bloque se ha modificado para reemplazar la "raíz global del estado" en el encabezado del bloque con la "raíz global pública del estado"
- El estado “Patricia Trie” se ha dividido en dos: un estado público y un estado privado.
- Se ha modificado la lógica de validación de bloques para manejar 'transacciones privadas'
- La creación de transacciones se ha modificado para permitir que los datos de transacciones sean reemplazados por hashes cifrados para preservar los datos privados cuando sea necesario

[16] Go Ethereum es una de las tres implementaciones originales (junto con C ++ y Python) del protocolo Ethereum. Está escrito en Go, de código abierto y con licencia bajo GNU LGPL v3.

[17] Geth es un cliente liviano de Ethereum

- El precio del gas se ha eliminado, aunque el gas sigue siendo el mismo.

Existen dos implementaciones de Quorum: Constellation desarrollada en Haskell[18] y Tessera implementado en Java. Son comparables a una red de MTA (agentes de transferencia de mensajes) donde los mensajes se cifran con PGP (Pretty Good Privacy). No es específico de una blockchain y es potencialmente aplicable en muchos otros tipos de aplicaciones, en las que se desea un intercambio de mensajes sellados individualmente dentro de una red de contrapartes.

El administrador de transacciones de Quorum es responsable de la privacidad de las transacciones, ya que almacena y permite el acceso a datos de transacciones encriptados; intercambia cargas encriptadas con los gestores de transacciones de otros participantes, pero no tiene acceso a ninguna clave privada sensible.

Los protocolos de libro mayor distribuido generalmente aprovechan las técnicas criptográficas para la autenticidad de la transacción, la autenticación del participante y la conservación de datos históricos (es decir, a través de una cadena de datos criptográficamente procesados). Para lograr una separación de actividades, así como para proporcionar mejoras en el rendimiento, Quorum usa esquemas de paralelización criptográfica. En las operaciones, gran parte del trabajo criptográfico, incluida la generación de claves simétricas y el cifrado/descifrado de datos, se delega la responsabilidad en un módulo de coordinación denominado “enclave”. Este módulo trabaja con el “transaction manager” para administrar el cifrado/descifrado de manera aislada, conteniendo claves privadas; operando como un módulo de seguridad.

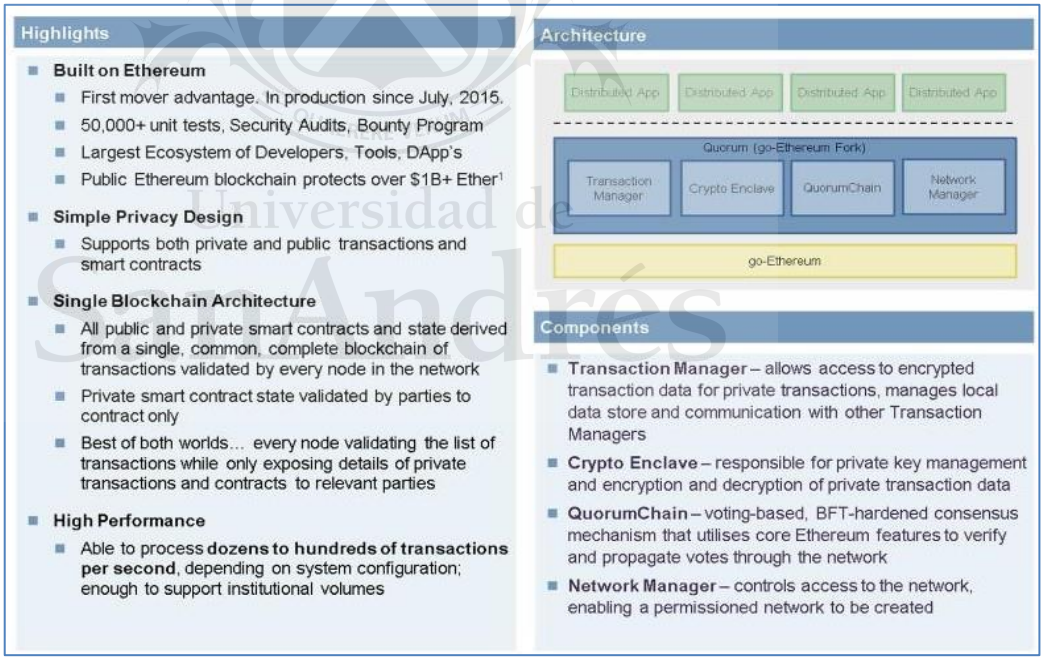


Ilustración 12 - Quorum Overview (Quorum Whitepape, 2016)

Una de las características relevantes de Quorum, es la privacidad de transacción. Para ello, introduce la noción de 'transacciones públicas' y 'transacciones privadas'.

Las "transacciones públicas" son aquellas transacciones cuya carga útil es visible para todos los participantes de la misma red de Quorum. Estas se crean como transacciones estándar de Ethereum

[18] Haskell es un lenguaje estándar multi-propósito.

de la manera habitual. Los ejemplos de transacciones públicas pueden incluir actualizaciones de datos de mercado de algún proveedor de servicios o alguna actualización de datos de referencia, como una corrección a una definición de bond security. Las transacciones 'públicas' no son transacciones de la red pública Ethereum. Se ejecutan de la manera estándar de Ethereum, por lo que si una transacción pública se envía a una cuenta que tiene un código de contrato, cada participante ejecutará el mismo código y se actualizarán en consecuencia.

Las "transacciones privadas" solo son visibles para los participantes de la red cuyas claves públicas están especificadas en un parámetro (privateFor) de la transacción. Este parámetro puede tomar varias direcciones separadas por coma. Se ejecutan según el estándar Ethereum: antes de que el nodo de Quorum del remitente propague la transacción al resto de la red, reemplaza la carga útil de la transacción original con un hash de la carga útil cifrada que recibe de Constellation o Tessera. Los participantes que son parte en la transacción podrán reemplazar el hash con la carga útil real a través de su instancia de Constellation o Tessera, mientras que los participantes que no son parte solo verán el hash. El resultado es que si se envía una transacción privada a una cuenta que tiene el código del contrato, los participantes que no son parte de la transacción simplemente terminarán omitiendo la transacción y, por lo tanto, no ejecutarán el código del contrato.

Quorum ofrece múltiples mecanismos de consenso, que pueden ser más apropiados según las necesidades del consorcio. Los más utilizados son:

- Consenso basado en RAFT[19]: un modelo de consenso para tiempos de bloque más rápidos, con finalidad de obtener mayor rendimiento en las transacciones y creación de bloques a pedido.
- Consenso basado en Estambul BFT (Tolerancia a fallos bizantinos)[20]: un algoritmo de consenso inspirado en PBFT (Practical BFT) destinado al mismo fin.

La seguridad en Quorum, se basa en los permisos de red, es decir que se controla qué nodos pueden conectarse entre sí.

Universidad de SanAndrés

Hyperledger

Hyperledger se creó para impulsar blockchain para las empresas (Hyperledger, 2018). En 2015, varias empresas interesadas en la tecnología blockchain/DLT, se dispusieron a aunar esfuerzos para desarrollar en esta tecnología una solución de código abierto y bajo licencia open source, lo que implica que cualquier empresa puede descargar, ver y cambiar. Bajo la tutela de la Fundación Linux, Hyperledger ha registrado un fuerte crecimiento, teniendo a la fecha más de 230 organizaciones miembros, entre los que se encuentran: ConsenSys, R3, Cisco, Digital Asset Holdings, Fujitsu, Hitachi, IBM, Intel, NEC, Red Hat, VMware, ABN AMRO, ANZ Banco, BNY Mellon, Grupo CLS, The Depository Trust & Clearing Corporation (DTCC), Grupo Deutsche Börse, J.P. Morgan, State Street, SWIFT, Wells Fargo, Accenture, Airbus, etc. ; dando un gran impulso para que blockchain se convierta en una tecnología popular y estándar en la industria. (Wikipedia, 2020)

[19] Raft es un algoritmo de consenso que es tolerante a fallos y posee buen rendimiento. (Bakhoff, 2014)

[20] Istanbul BFT, o IBFT, es una implementación del algoritmo Practical Byzantine Fault Tolerance con modificaciones, en que cada bloque requiere múltiples rondas de votación por parte del conjunto de validadores para llegar a un acuerdo mutuo. (Zhang, 2018)

Los beneficios claves para que las empresas se sumen a esta iniciativa de software de código abierto, encontramos:

- Características y capacidades competitivas
- Sin bloqueo de proveedores, por lo que los clientes pueden cambiar fácilmente
- Alta calidad de soluciones
- La capacidad de personalizar y corregir errores, a través del acceso al código fuente
- Menor costo total de propiedad

Hyperledger es neutral para los proveedores y cada empresa implementa blockchain internamente, utilizando los productos y servicios basados en proyectos Hyperledger. El código de Hyperledger es "interoperable", es decir puede trabajar con otros programas, incluso los implementados en otras organizaciones. Hyperledger Quilt es una framework, diseñado expresamente para admitir transacciones entre diferentes cadenas de blockchain.

Las empresas disponen de plataformas de blockchain Hyperledger modulares robustas, ricas en funciones que puedan personalizar para satisfacer sus necesidades. Las industrias como bancos, fabricantes de automóviles y aviones, financieras, etc. conforman un amplio “ecosistema de empresas”, cooperando todas en una comunidad global de desarrolladores y colaboradores de Hyperledger. Este consorcio de usuarios y proveedores diferentes colaborando para desarrollar la tecnología en conjunto, permite que todos puedan beneficiarse de un menor riesgo, mayor calidad y un tiempo de comercialización más rápido. Hyperledger es como un "invernadero" (greenhouse) que protege a los usuarios, desarrolladores y proveedores de diferentes sectores y espacios de mercado, que tienen como objetivo aprender, desarrollar y usar blockchain empresariales.

Como cada industria o empresa necesita características y modificaciones especiales, nunca habrá una única solución estándar de cadena de bloques; y Hyperledger proporciona una estructura de “invernadero” donde pueden incubar nuevas ideas, apoyar a cada una con recursos esenciales y distribuir los resultados ampliamente. Una estructura de esta característica puede soportar muchas alternativas diferentes, consumiendo muchos menos recursos.

Este tipo de organización para el desarrollo de blockchain de código abierto, ofrece estos beneficios:

- Ayuda para mantenerse al día con los desarrollos
- Mejor productividad a través de la especialización
- Colaboración para evitar esfuerzos duplicados
- Mejor control de calidad del código
- Manejo más fácil de la propiedad intelectual

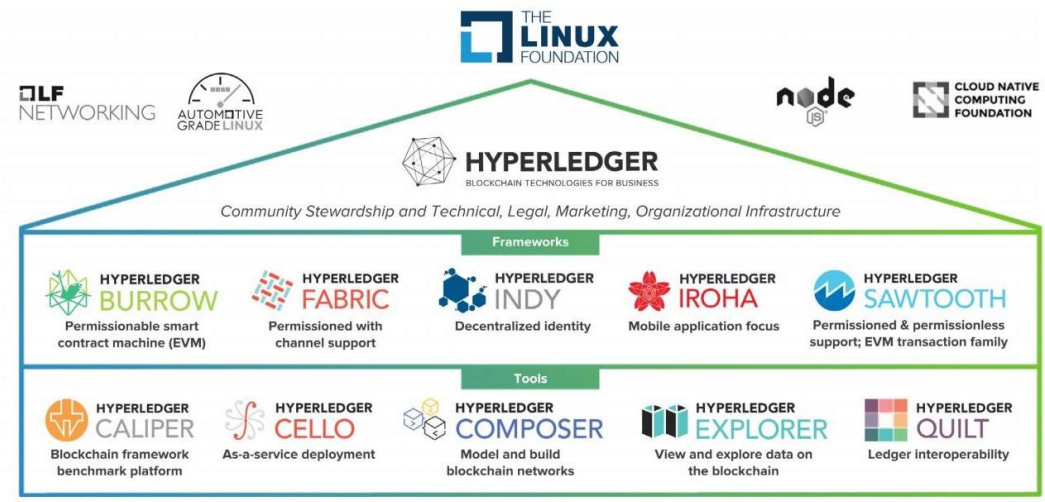


Ilustración 13 – La estructura invernadero de Hyperledger

Los principales frameworks y herramientas de Hyperledger (Wikipedia, 2020) son:

Hyperledger Burrow: Inicialmente impulsado por la startup Monax Industries y patrocinado por Monax e Intel. Es una cadena de bloques privada basada en el código de Ethereum. Permite el desarrollo de contratos inteligentes desarrollados en Solidity.

Hyperledger Fabric: Es uno de los proyectos de Hyperledger más conocidos, inicialmente impulsado e implementado por IBM y Digital Asset, aunque la comunidad de desarrolladores ha ido creciendo. Es una cadena de bloques de carácter privado y está orientada al uso empresarial gracias a la capacidad de realización de transacciones privadas. Tiene una arquitectura modular con una definición de roles entre los nodos de la infraestructura. Ha sido diseñada para ser una plataforma multidisciplinaria, es decir, permite la creación de contratos inteligentes (llamados chaincode en Fabric) en cualquier lenguaje. Por defecto en los inicios a la hora de implementar estos contratos inteligentes se utilizaba el lenguaje de programación de Google (Golang), pero con las sucesivas versiones se añadió el poder implementarlos en la versión 1.3 de NodeJS, lo que permitió implementarlos en Java. También es posible implementarlos en JavaScript (con Hyperledger Composer). Hyperledger Fabric está orientado principalmente para proyectos de integración para lo cual se necesita una tecnología de DLT, contando con el SDK para Go, Java y NodeJs.

Hyperledger Indy: Cadena de bloques diseñada especialmente para dar apoyo a ledgers con identidad descentralizada. Proporciona herramientas, librerías y componentes reutilizables para proveer identidades digitales basadas en la cadena de bloques o en otros ledgers distribuidos de modo que sean interoperables en distintos dominios administrativos y aplicaciones.

Hyperledger Grid: Este framework es un ecosistema de tecnologías, otros frameworks y librerías que trabajan juntos, dejando así elegir a los desarrolladores de aplicaciones que componentes son los más apropiados para su modelo de negocio.

Hyperledger Iroha: Esta cadena de bloques está diseñada para poderse incorporar fácilmente a otros proyectos. Está muy orientada al desarrollo de aplicaciones móviles. Tiene un tipo nuevo de consenso asíncrono de una fase del tipo de tolerancia a faltas bizantinas (BFT). Está desarrollado por Soramitsu, NTT Data y Colu.

Hyperledger Sawtooth: Impulsado por Intel, es un framework modular que permite crear y ejecutar cadenas de bloques altamente configurables, incluye una herramienta de consenso dinámica que permite realizar cambios rápidos de algoritmos de consenso, entre diversas opciones de consenso, siendo la más conocida la llamada PoET (Proof of Elapsed Time). Sawtooth apoya los contratos inteligentes de Ethereum via "seth"(un procesador de transacciones de Sawtooth integrado en la Máquina Virtual de Ethereum de Hyperledger Burrow). Proporciona SDKs para Python, Go, JavaScript, Rust y C++.

Hyperledger Caliper: Herramienta de benchmarking para plataformas de la cadena de bloques. Analizará el grado de rendimiento de cualquier plataforma de cadena de bloques en función de un conjunto de casos de uso predefinidos. Produce informes con indicadores de rendimiento como transacciones por segundo, la latencia de la transacción, etc... El objetivo de Caliper es usar los datos obtenidos como resultado para utilizarlos como base en otros proyectos, usando estos datos como referencia a la hora de elegir una implementación de la cadena de bloques que se ajuste a las especificaciones utilizadas. Estuvo impulsada inicialmente por Huawei, Oracle, Bitwise, Soramitsu, IBM y la universidad de Budapest de Tecnología y Economía.

Hyperledger Cello: Modulo de herramientas para la implementación de una cadena de bloques como un servicio. Reduce el esfuerzo para crear, terminar y administrar los servicios de la cadena de bloques. Desarrollada inicialmente por IBM al que se sumaron Intel, Soramitsu y Huawei posteriormente.

Hyperledger Composer: Ofrece un marco de desarrollo y un conjunto de herramientas para agilizar la implementación de aplicaciones de la cadena de bloques. Desarrollado en JavaScript, aprovechando herramientas modernas como NodeJs, npm, CLI y editores populares. Hyperledger Composer ofrece abstracciones centradas en el negocio, así como apps de muestra que ayudan al desarrollo de robustas cadenas de bloques que comprendan una mezcla entre los requisitos del negocio con los desarrollos tecnológicos.

Hyperledger Explorer: Impulsado por la Fundación Linux, está diseñado de manera que la aplicación web, sea simple y amigable para el usuario, se pueden ver, mostrar y listar nodos, bloques, estadísticas, transacciones, contactos inteligentes y muchos más.

Hyperledger Quilt: Es una herramienta de la cadena de bloques orientada a los negocios que ofrece interoperabilidad entre sistemas de registros distribuidos que utilizan el Inter Ledger Protocol. (ILP)[21]

Hyperlerger Ursa: Es una librería flexible, modular y compartida de criptografía. Permite evitar que se duplique el trabajo de encriptado e incrementar la seguridad en el proceso. Ursa consiste en un conjunto de sub-poyectos que son un conjunto de implementaciones cohesivas de código encriptado o de interfaces para encriptar código. Hay actualmente dos sub-proyectos llamados librería "Base Crypto" y “Z-Mix”.

Hyperledger Besu, de código abierto (similar Ethereum Pantheon) desarrollada por la *startup* de Ethereum ConsenSys, para lograr compabilidad entre Hyperledger/Ethereum.

Hyperledger Transact: tiene como objetivo reducir el esfuerzo de desarrollo en la escritura de software DLT al proporcionar una interfaz estándar para ejecutar contratos inteligentes que es

[21] El Protocolo Interledger (ILP), se basa en gran medida en el Protocolo de Internet (IP) y es un protocolos de pago descentralizados. El trabajo fue iniciado en 2004 por Ryan Fugger, aumentado por el desarrollo de Bitcoin en 2008 y desde entonces ha involucrado a numerosos colaboradores. (Wikipedia)

independiente de la implementación del libro mayor distribuido. Adopta un enfoque extensible para implementar nuevos lenguajes de contratos inteligentes llamados "motores de contratos inteligentes", que implementan una máquina virtual o un intérprete que procesa contratos inteligentes.

Hyperledger Avalon, es una implementación independiente de Trusted Compute Specifications publicada por la Enterprise Ethereum Alliance. Su objetivo es permitir el movimiento seguro del procesamiento de blockchain fuera de la cadena principal a recursos informáticos dedicados. Avalon está diseñado para ayudar a los desarrolladores a obtener los beneficios de la confianza computacional y mitigar sus inconvenientes.

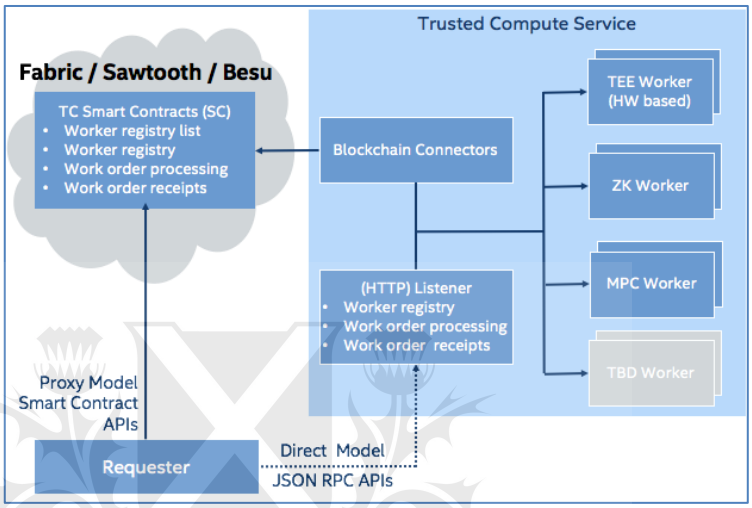


Ilustración 14 - Trusted Compute Service ((Hyperledger Avalon, 2019)

La filosofía detrás de Hyperledger, subyacen los siguientes principios:

- Modulares
- Altamente seguros
- Interoperables
- Independientes de alguna criptomoneda
- Completo con APIs

Ilustración 15 - La filosofía de diseño de Hyperledger

En general Hyperledger es un excelente conjunto de herramientas de base de datos distribuidas, que es comparable en arquitectura a las bases de datos distribuidas clásicas. Es básicamente un sistema monolítico, de enorme modularidad y posibilidades de customización, lo que conlleva un alto esfuerzo de configuración y administración. Hyperledger es particularmente adecuado para los casos de uso que requieren que los datos se intercambien con alto rendimiento entre un grupo cerrado de empresas. Hyperledger tiene limitaciones para crear aplicaciones distribuidas reales, ya que carece de una capa de tokenización, como para posibilitar un modelo de negocios descentralizado basados en activos digitales.

Red POA

La red POA es una red abierta, pública, permisionada basada en el protocolo Ethereum, con tipo de consenso de Prueba de Autoridad (PoA), lo cual es implementado mediante nodos validadores independientes previamente seleccionados. Esta red permite la escalabilidad de la cadena de bloques, en forma horizontal mediante la interconexión con otras cadenas de bloques con consenso de la Prueba de Autoridad, que sean admitidas. El diseño de este ecosistema tiene el potencial de resolver los problemas de velocidad de las transacciones, rendimiento de la cadena de bloques y costo de las redes. (Perez, Isabel, 2020)

POA Network intenta resolver el problema del costo derivado del uso de las redes públicas (Bitcoin o Ethereum), al tiempo que mejora su velocidad; haciendo que la plataforma de contrato inteligente sea más barata y más rápida que las tradicionales de Proof of Work (PoW).

La Prueba de Autoridad (PoA) es una forma sencilla y eficiente de prueba de participación, que utiliza un conjunto de "autoridades", nodos a los que se les permite explícitamente crear nuevos bloques y confirmar el blockchain. (Kovan) ejecutando el algoritmo de consenso de PoA.

En PoA, no se requiere que los nodos validadores mantengan una participación permanente en la red; sin embargo, debe poseer una identidad conocida y verificada. Conocer la identidad de los nodos validadores, desincentiva que actúe de manera maliciosa o se confunda con otros validadores. Cualquier nodo malicioso puede ser eliminado y reemplazados. Las garantías legales existentes contra el fraude se utilizan para proteger a los participantes de la red abierta de acciones malintencionadas de validadores.

En la Red de POA, el consenso de PoA se basa en el tipo especial de validadores independientes. En Estados Unidos, se requiere que cada uno de ellos tenga una licencia de notario público activa dentro de los Estados Unidos. Los notarios públicos se someten a verificación a través de las solicitudes de identidad de la red de POA, seguido de la ceremonia de inicio para recibir las claves, lo que les permite asegurar la red. Cualquier nueva red especializada en la parte superior de la red de POA puede usar los mismos validadores o tener su propio conjunto de validadores con cualquier otro tipo de licencia verificable.

La capa central de la Red de POA está compuesta inicialmente por doce nodos (personas respetables) que protegen la red. Está diseñado como un blockchain de aplicación general. Es decir, todo lo que se puede hacer en la red Ethereum, también se puede hacer en la red POA. Las organizaciones pueden construir de forma rápida y económica otras redes especializadas en la parte superior con el mismo o diferente conjunto de validadores, según la ceremonia y el gobierno de la Red de POA. Los

desarrolladores pueden implementar DApps utilizando la red POA; siendo interoperables utilizando una pasarela con Ethereum.

BFA (Blockchain Federal Argentina)

BFA (Blockchain Federal Argentina) es una plataforma multiservicios de alcance federal basada en blockchain, conformada por un consorcio de actores del sector público, privado, técnicos, académicos y de la sociedad civil. Este marco de colaboración *multistakehoder* es el que marca el modelo de gobernanza y gestión de la red, buscando integrar a los diferentes sectores en la estructura de gestión del consorcio y en la gestión de la arquitectura técnica y operativa que permite el funcionamiento de la blockchain. (BFA, 2020)

La red de BFA es un clon del código de Ethereum, pero adoptando como mecanismo de consenso la Prueba de Autoridad (PoA). Es una red permisionada, que contempla la habilitación de 26 nodos selladores que son los únicos que pueden validar los bloques. Los nodos selladores, pasan por un proceso de habilitación, lo que incluye la certificación de la identidad.

El ecosistema, permite a los desarrolladores crear y publicar aplicaciones distribuidas para ejecutar "smart contracts" garantizados por la cadena de bloques. La red posee una infraestructura de nodos a nivel global. Como el desarrollo está basado en código abierto, toda la comunidad puede participar en las pruebas de concepto existentes para mejorar la plataforma, o tomar todo ese trabajo y adaptarlo a otros contextos y necesidades.

Al estar la red estructurada en un entorno confiable y con un mecanismo de consenso eficiente como PoA, resulta eficiente en lo relativo a cantidad de transacciones por unidad de tiempo, consumo eléctrico y costo de operación.

En la forma en que está estructurada la red, no es necesaria la implementación de una moneda virtual para aprovechar las ventajas que blockchain nos proporciona, por eso BFA está diseñada específicamente para no poseer criptomoneda asociada. Se optó por un modelo de consenso que no se alimenta de la competencia entre las partes. "El incentivo para participar en BFA no es la acumulación de moneda virtual, no es la ganancia, sino favorecer el desarrollo de servicios e iniciativas basadas en la innovación tecnológica y en un trabajo horizontal entre diversos actores".

La utilización de la BFA es pública y no está restringida a las organizaciones que participen del consorcio. Las organizaciones que deseen desarrollar servicios y/o aplicaciones distribuidas sobre la blockchain deberán aceptar un acuerdo de utilización y buenas prácticas, pero no estarán obligados a desplegar nodos validadores. BFA se encargará de la infraestructura mientras que los usuarios desarrollarán las aplicaciones.

Universidad de San Andrés

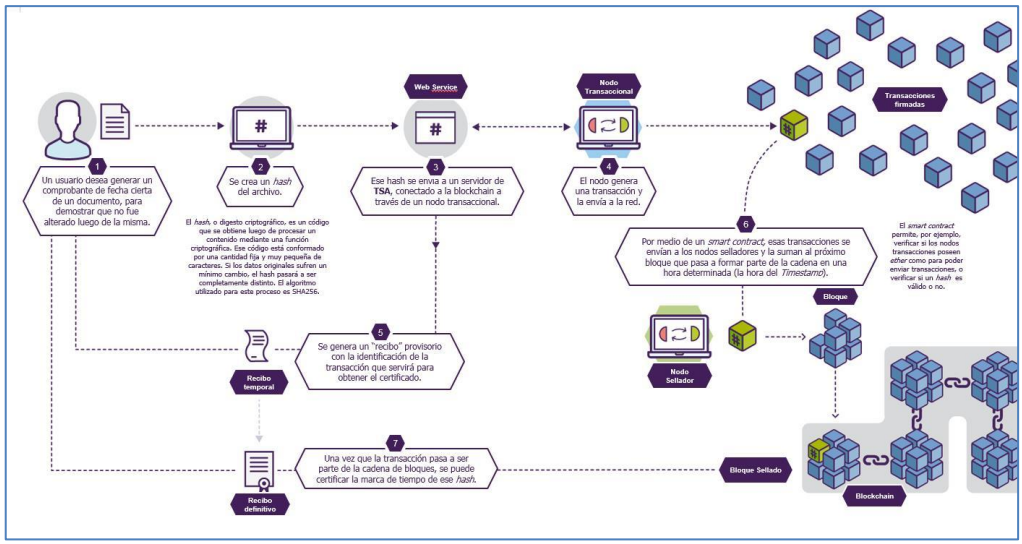


Ilustración 16 – Esquema de red BFA (BFA, 2020)

La red está integrada por distintos tipos de nodos:

- Los nodos selladores (o *sealers*) conforman la estructura central de la red confiable de BFA ya que son los únicos que pueden sellar (agregar) bloques a la cadena. Todos ellos están desplegados por miembros del consorcio. Los selladores están conectados solamente entre sí, y a los nodos tipo Gateway, que actúan como buffer entre ellos y el resto de la red. Los nodos transaccionales (*transaction nodos*) son aquellos que pueden enviar transacciones, para que luego sean procesadas por los nodos selladores. Usualmente son ejecutados por operadores de servicios que utilizan la blockchain (los que implementan aplicaciones) .
- Existen también nodos verificadores (*read-only*), que pueden "ver" la blockchain, pero no pueden generar ni sellar transacciones. Cualquier usuario puede correr este tipo de nodos, sin necesidad de autorización de BFA.

La eficiencia del modelo de Prueba de Autoridad habilita que los nodos selladores no se requieran servidores con gran capacidad de procesamiento (4vCPU, 8GB de RAM y 1TB de HD). Los nodos de los operadores de servicios no poseen requerimientos mínimos, y deberán ajustarse solamente a las necesidades de los mismos.

Para enviar transacciones a la blockchain se necesita un “combustible”. Este toma forma de *tokens* virtuales llamados *Ether (o gas)* que BFA distribuirá a aquellos operadores de nodos transaccionales que desplieguen aplicaciones sobre la plataforma. Los mismos no tienen ningún tipo de valor económico y se envían periódicamente mediante una *destilería* operada por el consorcio.

Se implementa un modelo donde se evita la especulación y/o el tráfico de *tokens*, además de habilitar la implementación de métodos para detectar el abuso. Al mismo tiempo, para reafirmar la transparencia, un nodo validador (así como cualquier otro que se integre a la red) podrá verificar la fidelidad de la información, sin necesidad de poseer *tokens* para realizarlo.

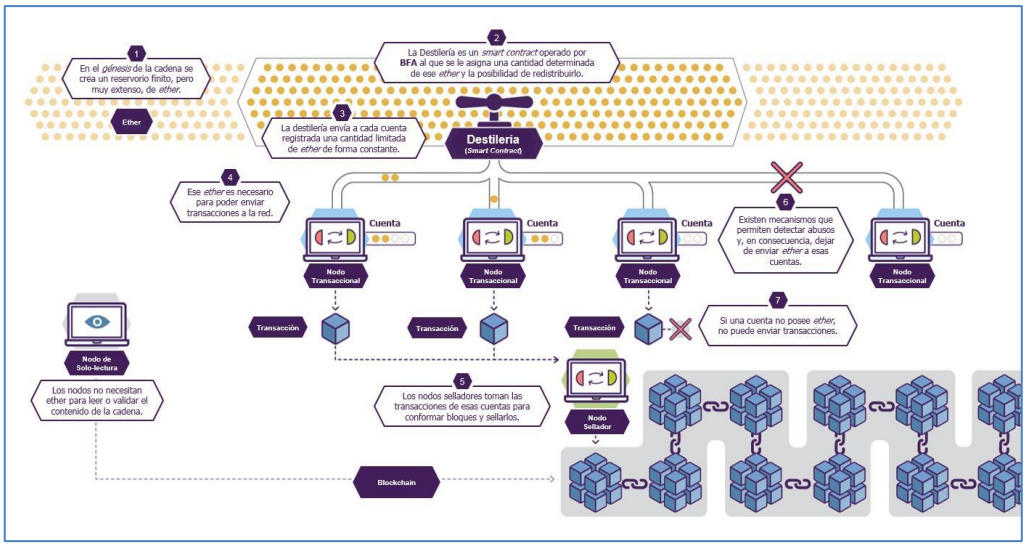


Ilustración 17 - Destilería de BFA (BFA, 2020)

El software de Blockchain Federal Argentina se basa en una implementación abierta y robusta. Todos los desarrollos y modificaciones que se realicen serán igualmente abiertos, de modo que puedan ser públicamente auditados por cualquier interesado, más allá de los participantes del consorcio. La transparencia inherente en el modelo queda también garantizada desde el código.

Cada entidad que administre un nodo de BFA es responsable del mantenimiento y monitoreo. De hecho no existe en la red un sistema central de administración. Como apoyo, Blockchain Federal Argentina sí implementará un esquema de nodos de monitoreo a través del NOC (*Network Operation Center*), que estará atento al normal funcionamiento de todos los nodos.

Existen modos de certificar contenidos a través de *blockchain*. Estos mecanismos permiten generar una "prueba de existencia", algo así como un sello digital que demuestra que un mensaje existía antes de una fecha y hora determinada.

El servicio de TSA (*Time Stamping Authority)* desarrollado por BFA permite demostrar o evidenciar que un determinado archivo digital se ha mantenido inalterado en el tiempo a partir de una determinada fecha.

El diseño, tanto técnico como de gestión de Blockchain Federal Argentina, no solo fue pensado para garantizar que la iniciativa fuera escalable gracias a la incorporación de nuevos participantes, sino también a asegurar su continuidad en el tiempo: que perdure más allá de las personas e instituciones que lo gestaron gracias a un modelo de trabajo horizontal y colaborativo.

La plataforma está diseñada pensando en una infraestructura que garantice la interoperabilidad y la sinergia entre emprendimientos similares en toda América Latina y el Caribe.

Todas las ventajas de esta tecnología se fortalecen al estructurarlas en torno a un proyecto participativo, que evoluciona y se fortalece a través de la incorporación de nuevos integrantes. Esta ambición por sumar nuevas partes es la que también garantiza la continuidad en el tiempo de BFA: que perdure más allá de las personas e instituciones que lo gestaron gracias a un modelo de trabajo multisectorial y distintos actores involucrados.

BFA es una iniciativa que intenta consolidar una herramienta colaborativa y de vanguardia, que funcione como soporte de ideas para empresas e instituciones; pretendiendo ser el primer espacio digital común de estas características en Argentina: un ecosistema ideal para productos y servicios que busquen una infraestructura sólida, abierta, transparente y confiable.

Finalmente, rescatamos que la Prefectura opera un nodo sellador de esta red desde 2018, junto a otros organismos, universidades y empresas u organizaciones que están comprometidas con el desarrollo de esta tecnología. La red a la fecha se encuentra totalmente operativa y presta servicios relevantes como: sellado del Boletín Oficial de la RA; validación de títulos del Ministerio de Educación, Sistema de Documentos Notariales Digitales (GEDONO) del Colegio de Escribanos de la Ciudad de Buenos Aires y Carpeta Ciudadana del Gobierno de la Ciudad de Buenos Aires.

Nodos selladores

Nombre	Total Bloques Sellados	Último Bloque	Time Stamp
Colescribanos	202472	9704285	hace 5 minutos
PNA / Prefectura Naval Argentina	498669	9704284	hace 5 minutos
UP / Universidad de Palermo	345939	9704283	hace 5 minutos
SRT / Superintendencia de Riesgos del Trabajo	366589	9704282	hace 5 minutos
ASI / Agencia de Sistemas de Información, CABA	525376	9704281	hace 5 minutos
UNP / Universidad Nacional de La Plata	467023	9704280	hace 5 minutos
DGSI / Dirección General de Sistemas de Información	493976	9704279	hace 5 minutos
UM / Ultima Milla SA	190415	9704278	hace 5 minutos
ARIU / Asociación Redes de Interconexión Universitaria	516759	9704277	hace 5 minutos
ANSV / Agencia Nacional de Seguridad Vial	241480	9704276	hace 5 minutos
UNSJ / Universidad Nacional de San Juan	461005	9704275	hace 5 minutos
CABASE PMY / CABASE Puerto Madryn	271337	9704274	hace 6 minutos
IXPBB / IXP Bahia Blanca	451905	9704273	hace 6 minutos
UNER / Universidad Nacional de Entre Ríos		9704272	hace 6 minutos
Red Link	246488	9704271	hace 6 minutos
CABASE BUE / CABASE CABA	476549	9704270	hace 6 minutos
CABASE PSS / CABASE Posadas	66170	9704268	hace 6 minutos
UNC / Universidad Nacional de Córdoba	483290	9704267	hace 6 minutos
CABASE MZA / CABASE Mendoza	318879	9704266	hace 6 minutos
ONTI / Oficina Nacional de Tecnologías de Información	474039	9704265	hace 6 minutos
UNR / Universidad Nacional de Rosario	465540	9704264	hace 6 minutos
Marandú	313765	9704262	hace 7 minutos
SMGP/OPTIC	295810	9704261	hace 7 minutos
IPLAN	198207	8582204	hace 2 meses
Everis	296967	6074590	hace 7 meses

Ilustración 18 - Nodos selladores (http://bfascan.com.ar/selladores)

Universidad de SanAndrés

3 – Aspectos Legales:

El Registro Nacional de Buques

El Registro Nacional de Buques, fue creado por el Decreto-Ley 18300/56, bajo la órbita de la Prefectura Naval Argentina, con el nombre de Registro General de la Propiedad Naval y es la autoridad de aplicación en materia de publicidad registral en el ámbito naval. Su actual Ley Orgánica es la N° 19170 y está reglamentada por la Ordenanza Marítima N° 9/02, conforme a lo dispuesto por el artículo 46, por el cual se delegó esa facultad en el Prefecto Nacional Naval.

El Registro Nacional de Buques, se basa en el siguiente marco normativo:

- Ley 18.398: determina la dependencia orgánica del RNBU de la Prefectura.
- Ley 19.170 –Ley Orgánica del Registro Nacional de Buques-
- Ley 20.094 –Ley de la Navegación- que le otorga al Registro Nacional de Buques facultades organizativas.
- Decreto 4516/73, Régimen de la navegación marítima, fluvial y lacustre, reglamentario de la ley 20.094.
- Ordenanza Marítima N° 9/02, reglamentaria de la Ley del Registro.
- Otras normas modificatorias y/o complementarias.(Disposición 1363/2018)

Este Registro Nacional, en virtud del principio registral de inscripción, como registro jurídico de cosas, cumple dos funciones interrelacionadas entre sí, la matriculación y el registro de buques.

- La obligatoriedad de la matriculación, surge de la Ley 19170 y resulta indispensable para estructurar el sistema registral dominial, que funciona sobre la base del Folio Real y tiene por objeto dotar al buque y al artefacto naval de nacionalidad argentina. Esto le otorga el uso del pabellón y lo pone bajo el amparo de la legislación nacional.
- El registro, se realiza sobre la base de la matriculación y consiste en la inscripción del dominio y sus afectaciones, ya sea que provengan de derechos reales de garantía, derechos reales de disfrute, derechos personales (en los casos que la ley lo determina) o medidas cautelares en aras de asegurar el tráfico jurídico.

La matriculación vinculada con el poder de policía de seguridad de la navegación del Estado, se rige por normas de derecho público de la navegación; mientras que la registración, es el ejercicio del poder de policía de la propiedad del Estado y las normas que la regulan integran el derecho privado de la navegación.

El acto jurídico de la matriculación, confiere nacionalidad al buque matriculado y torna inadmisible la posibilidad de una doble bandera. Si esta situación se diera, implicaría la imposibilidad jurídica de ampararse en ninguna de las dos. “Tal solución, resulta a todas luces lógica, y no debemos olvidar que el derecho es lógica aplicada, ya que la circunstancia arriba indicada, resultaría un gravísimo atentado contra la seguridad jurídica. La esencia de todo registro de bandera y de propiedad radica en la preservación de la seguridad jurídica y de la navegación”. (Acha, 2013)

Son funciones del Registro Nacional de Buques:

- Llevar el Registro de la Matrícula Nacional; que comprenderá el de la Matrícula Mercante Nacional y el Registro Especial de Yates, donde se inscribirán obligatoriamente los buques y artefactos navales de propiedad estatal o privada que determine la reglamentación.

- Tomar razón de todo documento por el que se constituya, transmita, declare, modifique o extinga derechos reales sobre buques o artefactos navales que pertenezcan a la matrícula nacional.
- Tomar razón de todo documento que disponga embargos, interdicciones o cualquier otra afectación de dominio que recaiga sobre buques y artefactos navales, sea que pertenezcan a la Matrícula Nacional o extranjera.
- Tomar razón de todo documento por el que se prive a una persona de la libre disponibilidad de sus bienes, sea que resulte de un convenio voluntario entre partes o por resolución judicial.
- Llevar todo otro registro que por imperio de disposiciones legales se le asignen.
- Expedir todas las certificaciones que correspondan de los asientos contenidos en sus registros.
- Determinar el arancel que corresponda abonar por todas las tramitaciones que se efectúen ante el Registro, de acuerdo con las disposiciones vigentes en la materia.

La Matrícula Mercante Nacional, está formada por tres agrupaciones en las se inscriben con carácter obligatorio, todos los buques o artefactos navales:

- Primera Agrupación (Mayores): Buques de 10 o más toneladas de arqueo total[22], de propietarios privados y que se destinen al comercio o la pesca.
- Segunda Agrupación (Menores): Buques de 2 a 9 nueve toneladas de arqueo total, de propietarios privados y que se destinen al comercio o la pesca. Su número matricula va seguido de la letra M
- Tercera Agrupación (Fiscales): Buques mayores de 2 toneladas de arqueo total y cuyo propietario sea el Estado Nacional, Provincial o Municipal. El número de matrícula va seguido de la letra F.
- Registro Especial de Yates: Buques, de propietarios privados, destinados al deporte náutico, recreo o actividades vinculadas, mayores de 2 toneladas de arqueo total. El número de matrícula va seguido de la sigla REY.

El Registro Nacional de Buques se basa en el sistema registral declarativo y no convalidante de derechos; "… la función de registración que cumple el Registro Nacional de Buques, resulta importante destacar, que se ha estructurado sobre la base de un sistema registral declarativo y no convalidante de derechos, implementado mediante la técnica real. El sistema es de carácter declarativo en razón de que los derechos que se inscriben nacen fuera del registro, sumando para ello, modo suficiente (tradición de la cosa objeto del derecho real, cuando éste se ejerce mediante la posesión) y título suficiente (acto jurídico válido que reúne la totalidad de recaudos de fondo y de forma necesarios para transferir o constituir el derecho real que se pretende); salvo para el caso de los derechos reales de garantía (hipoteca y prenda naval), los que nacen tan sólo con el otorgamiento del título suficiente, ya que no se ejercen por la posesión. Por consiguiente, la registración resulta necesaria para otorgarle a los derechos reales o personales (que requieran de inscripción), previamente transferidos, adquiridos o constituidos, oponibilidad respecto de terceros interesados". (Acha, 2013)

"La implementación de un sistema no convalidante de derechos, determina que la inscripción de un derecho, no implica sanear al documento que lo contiene de los vicios de que pudiera adolecer. Si el documento resulta inscribible, se registra su contenido, sin perjuicio de que luego la validez de ese documento pueda ser discutida en sede judicial y, como resultado de una eventual sentencia favorable a la presentación efectuada, se ordene la variación o cancelación del asiento registral oportunamente practicado". (Acha, 2013)

[22] Por "Arqueo Bruto" se entiende el arqueo denominado y determinado como tal en la normativa vigente nacional e internacional. Dicho arqueo representa el "Arqueo Total" en los términos de la Ley 20.094

El registro se basa en la técnica de folio real y de inscripción, complementada mediante la sub-técnica de breves notas. "… la técnica de folio real se complementa adecuadamente con la técnica de registración mediante breves notas, la que resulta altamente conveniente, tanto para la toma de razón, como para la expedición clara, rápida y segura de la información registrada". (Acha, 2013)

El Registro es de carácter público, ello implica que podrá brindar la información que contiene en sus registros a toda persona que lo solicite por escrito, mediante los formularios establecidos por la reglamentación respectiva, pagando el arancel establecido y acreditando para ello un fundado interés legítimo. El Registro brinda esa información mediante la expedición de simples informes sin reserva de prioridad o certificados con reserva de prioridad indirecta. Estos últimos, sólo pueden ser solicitados por un escribano público, con carácter previo a la autorización de un acto por el que se transmitan, constituyan, modifiquen o cedan derechos reales sobre buques. Tal certificación con reserva de prioridad, tendrá una validez de 15 a 30 días, a partir de la cero hora del día de su expedición, según que el escribano solicitante tenga domicilio legal en la ciudad de Buenos Aires o en otra jurisdicción.

"Luego de otorgado el acto por las partes intervinientes, el escribano autorizante deberá presentar la primera copia o testimonio del documento, con la debida legalización por parte del Colegio Notarial respectivo, dentro de los 45 días posteriores, contados a partir de la firma del acto, a fin de poner en marcha el instituto de retro-prioridad, mediante el cual el derecho queda registrado a partir del día en que nació extra-registralmente, con los efectos de oponibilidad 'erga omnes'[23] para terceros desinteresados. Sin lugar a dudas la combinación de estos dos institutos jurídicos (la reserva de prioridad indirecta y la retro-prioridad) dotan a un negocio jurídico en gestación del mayor resguardo jurídico posible. El contenido de todo otro documento, de origen judicial, eventualmente administrativo, o notarial, que no se encuentre al amparo de una reserva de prioridad indirecta, será registrado con prioridad directa. Mediante la implementación de estos sistemas y técnicas registrales, el Registro Nacional de Buques, se convirtió en un registro jurídico modelo en toda Hispanoamérica, gracias al resguardo que está en condiciones de brindar a la seguridad jurídica". (Acha, 2013).

Modernización del Estado.

El proceso de modernización del Estado, es y ha sido en general uno de los objetivos permanentes y continuos de todos los gobiernos; teniendo en los últimos años quizás una mayor dinámica producto del acelerado desarrollo tecnológico alcanzado. Dentro de los instrumentos legales, normativos o instrumentales que podemos encontrar, resulta necesario destacar a los siguientes:

La Firma Digital

La firma digital fue establecida en la Argentina por Ley 25.506, promulgada en el año 2001, y establece las consideraciones generales sobre los certificados digitales; el certificador licenciado, la titularidad de un certificado digital, la organización institucional y su autoridad de aplicación; como así también el sistema de auditoría.

El objeto de esta ley es reconocer el empleo de la firma electrónica y de la firma digital y su eficacia jurídica.

[23] Locución latina, que significa "respecto de todos" o "frente a todos", utilizada en derecho para referirse a la aplicabilidad de una norma, un acto o un contrato.

En este sentido, indica que se entiende por "**firma digital"** al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes y que tal que dicha verificación, simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. Los procedimientos de firma y verificación utilizados para tales fines, deberán ser determinados por la autoridad de aplicación en consonancia con estándares tecnológicos internacionales oportunamente vigentes.

Subsidiariamente, señala que se entiende por "**firma electrónica**" al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación y que carezca de alguno de los requisitos legales para ser considerada firma digital. Aclara que para el caso, que la firma electrónica sea desconocida por su autor, corresponderá a quien la invoca acreditar su validez.

La firma digital presume autoría, esto implica que, salvo prueba en contrario pertenece al titular del certificado digital que permite la verificación de dicha firma. También se presume su integridad, es decir que salvo prueba en contrario, si el resultado de un procedimiento de verificación es verdadero, se presume que ese documento digital no ha sido alterado desde el momento de su firma. Para que una firma digital sea considerada válida debe cumplir con las siguientes condiciones: haber sido creada durante el período de vigencia del certificado digital válido del firmante; se encuentre debidamente verificada por la referencia a los datos de verificación del certificado y que ese certificado haya sido emitido o reconocido por un certificador licenciado.

Por "**documento digital**", se entiende a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo[24]. Un documento digital también satisface el requerimiento de escritura[25].

Existen dos posturas entre los profesionales del derecho en relación a la valoración de la firma electrónica. Por un lado, un postura más restrictiva, fundamenta que sola la firma digital posee la equiparación legal y jurídica de la firma ológrafa y en consecuencia, todo documento digital con firma electrónica corresponde sea considerado como un instrumento particular no firmado[26].

Esta discusión jurídica excede el alcance de este trabajo; y ambos tipos de firmas se encuentran alcanzados por la legislación; en cualquier caso, cabrá dirimir la fuerza probatoria de una firma electrónica en base a la infraestructura tecnológica que la soporte. Lo cierto es que existen hechos concretos de la efectiva valoración y profusa utilización que recibe la firma electrónica en diversos ámbitos; tal como lo indica (Bielli & Ordoñez, 2019) " al mencionar que "… la Ley 27.444, de 'Simplificación y Desburocratización para el Desarrollo Productivo de la Nación', que refiere a la firma electrónica en varios pasajes e incluso le reconoce, en algunos casos, idénticos efectos que a la firma digital, efectuando consagraciones normativas de gran relevancia en las Leyes 25.065 (Tarjeta de

[24] "...un documento digital es básicamente un registro (o una anotación, o una marca), y su particularidad radica en que se realiza mediante medios digitales y que se almacena en la memoria de un ordenador o en otros soportes similares". (Mora, 31/12/2013)

[25] La expresión escrita puede tener lugar por instrumentos públicos, o por instrumentos particulares firmados o no firmados, excepto en los casos en que determinada instrumentación sea impuesta. Puede hacerse constar en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos. (Art. 286 - Código Civil y Comercial).

[26] Los instrumentos particulares pueden estar firmados o no. Si lo están, se llaman instrumentos privados. Si no lo están, se los denomina instrumentos particulares no firmados; esta categoría comprende todo escrito no firmado, entre otros, los impresos, los registros visuales o auditivos de cosas o hechos y, cualquiera que sea el medio empleado, los registros de la palabra y de información.(Art. 287 - Código Civil y Comercial)

crédito) y 24.452 (Cheques), y en el Decreto-ley 5.965 (Letras de cambio y pagare). En tal sentido, incorpora en tales regímenes que, si el instrumento fuese generado por medios electrónicos, el requisito de la firma quedará satisfecho si se utiliza cualquier método que asegure indubitablemente la exteriorización de la voluntad de las partes y la integridad del instrumento".

El sistema de infraestructura de firma digital de la Argentina requiere de una única autoridad superior de confianza (autoridad certificante raíz) a través de la cual se termina validando todo el sistema. Esto lo vemos en los aspectos de la organización institucional de firma digital que establece que los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, por un certificador licenciado. La estructura de certificación que cuenta únicamente con dos (2) niveles, donde el primer nivel es el de la "Autoridad Certificante Raíz de la República Argentina", operada por la Jefatura de Gabinete de Ministros[27], y el segundo nivel correspondiente a las "Autoridades Certificantes" operadas por los certificadores licenciados. No hay autoridades certificantes subordinadas a estas últimas.

Conforme la doctrina especializada (Bielli & Ordoñez, 2019), para poder configurar una firma digital debe cumplirse indefectiblemente con los siguientes requisitos cardinales:

- En primer lugar, debe haber sido creada durante el período de vigencia del certificado digital válido del firmante.
- Debe ser debidamente verificada por la referencia a los datos de verificación de firma digital, indicados en dicho certificado según el procedimiento de verificación correspondiente. Es así que se debe permitir verificar la identidad del autor de los datos (lo que se denomina autenticación de autoría).
- Se debe poder comprobar que dichos datos insertos no han sufrido alteración desde que fueron firmados (proporcionándose integridad al documento electrónico).
- Por último, dicho certificado debe haber sido emitido o reconocido, según el art. 16 de la ley, por un certificador licenciado. Es así que el certificado de firma digital debe haber sido emitido por una entidad certificante licenciada por el Estado, obteniendo la correspondiente autorización por la autoridad de aplicación nacional.

El Decreto 182/2019[28], actualiza la reglamentación sobre la eficacia jurídica del documento electrónico, de la firma electrónica y la firma digital; complementando normas de derecho civil y comercial relativas a la firma, al documento, a su condición de original y a la conservación documental, elementos esenciales para otorgar seguridad a las transacciones electrónicas, promoviendo el comercio electrónico seguro y la autenticación fehaciente de las personas que realizan dichas transacciones en entornos virtuales.

Dicha norma, asimismo establece medidas de simplificación administrativa y formalidades legales y modalidades de firma digital, como: firma digital remota, firma digital con dispositivo criptográfico externo (token) y firma digital con certificado del sistema, las cuales gozan de plena validez jurídica, asegurando indubitablemente la autoría e integridad del documento electrónico firmado digitalmente. Indica que la firma digital de un documento electrónico satisface el requisito de certificación de firma establecido para la firma ológrafa y que la exigencia legal de conservar documentos, registros o datos, queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente.

[27] La dependencia y denominación del organismo responsable de la autoridad certificante raíz de la argentina, ha tenido numerosos cambios.

[28] Actualización de la reglamentación de la Ley de Firma Digital (Ley N° 25.506 y su modificatorias)

Por otra parte establece que los documentos, registros o datos electrónicos, deberán ser almacenados por los intervinientes o por prestadores de servicios de confianza[29] aceptados por los intervinientes, durante los plazos establecidos en las normas específicas; debiendo la conservación de documentos, registros o datos en formato electrónico garantizar su integridad, accesibilidad y disponibilidad.

En el Capítulo II del Anexo a este decreto, se establece que componen la Infraestructura de Firma Digital en los términos establecidos por la Ley:

- La Autoridad Certificante Raíz de la República Argentina.
- El Ente Licenciante.
- Los certificadores licenciados, incluyendo sus autoridades certificantes y sus autoridades de registro, según los servicios que presten.
- Las autoridades de sello de tiempo.
- Los suscriptores de los certificados.
- Los terceros usuarios.
- Los certificadores reconocidos por la Autoridad de Aplicación.
- El Organismo Auditante (Sindicatura General de la Nación).
- Los prestadores de servicios de confianza.

Acá se destacan dos figuras: las autoridades de sello de tiempo y los prestadores de servicios de confianza; los cuales están íntimamente ligados a la tecnología blockchain.

A tal efecto determina que se entiende por "servicio de confianza", al servicio electrónico prestado por un tercero de confianza relativo a:

- La conservación de archivos digitales.
- La custodia de declaraciones de voluntad realizadas en formato electrónico, contratos electrónicos, y toda otra transacción que las partes decidan confiar a un tercero depositario.
- La notificación fehaciente de documentos electrónicos.
- El depósito de declaraciones de voluntad realizadas en formato electrónico.
- **La operación de cadenas de bloques para la conservación de documentos electrónicos, gestión de contratos inteligentes y otros servicios digitales.**
- Los servicios de autenticación electrónica.
- Los servicios de identificación digital.
- Otras prestaciones que determine el Ente Licenciante.

Los Servicios de Confianza, pueden brindar su servicio a personas humanas, jurídicas, consorcios, entes públicos, entes públicos no estatales, de acuerdo a los procedimientos, estándares y condiciones que determine la autoridad de aplicación.

[29] "...sistemas informáticos accesibles vía web, ya sean públicos o privados, que mediante la implementación de tecnologías tales como la firma electrónica y el sellado de tiempo (timestamp) – en forma conexa y en atención a determinados estándares de seguridad- hacen las veces de certificadores y depositarios de documentos electrónicos pasibles de atestiguar la ocurrencia de hechos u actos jurídicamente relevantes suscitados en el mundo virtual y consecuentemente, revestirlos del necesario valor probatorio a fin de eventualmente procurar ser introducidos, como prueba instrumental, a un proceso judicial." (Bielli G. E., 2019)

Plan de Modernización del Estado

La modernización del Estado ha estado en la agenda de casi todos los gobiernos, pero lo cierto es que el mayor aporte hacia este objetivo se cristaliza en año 2016, con lo se denominó "Plan de Modernización del Estado" [30] y que ha introducido una serie de modificaciones normativas y acciones en concreto que permitieron un gran avance en esta materia.

El Plan de Modernización del Estado define los ejes centrales, las prioridades y los fundamentos para promover las acciones necesarias orientadas a convertir al Estado en el principal garante del bien común; abordando la problemática a partir de la instrumentación de un conjunto sistemático, integral y metódico de acciones concretas.

Entre los objetivos de este Plan de Modernización, se destacan muy especialmente:

- Incorporar nuevas tecnologías a la administración pública para que los trámites sean más fáciles, más rápidos y más seguros.
- Reducir la burocracia estatal y agilizar la interacción entre el Estado y los ciudadanos con una administración sin papeles.
- Implementar el expediente electrónico para despapelizar el Estado.
- Incorporar trámites a distancia.

El plan tiende a aumentar la calidad de los servicios provistos por el Estado incorporando Tecnologías de la Información y de las Comunicaciones, simplificando procedimientos, propiciando reingenierías de procesos y ofreciendo al ciudadano la posibilidad de mejorar el acceso por medios electrónicos a información personalizada, coherente e integral.

Dentro del citado marco, se estructuraron 5 ejes:

- Plan de Tecnología y Gobierno Digital:
- Gestión Integral de los Recursos Humanos
- Gestión por Resultados y Compromisos Públicos
- Gobierno Abierto e Innovación Pública
- Estrategia País Digital

De estos cinco ejes, rescatamos los dos directamente relacionados con el motivo de nuestro estudio:

- Plan de Tecnología y Gobierno Digital: Se propuso fortalecer e incorporar infraestructura tecnológica y redes con el fin de facilitar la interacción entre el ciudadano y los diferentes organismos públicos. Asimismo, se busca avanzar hacia una administración sin papeles, donde los sistemas de diferentes organismos interactúen autónomamente.

  Respecto de este punto, se dio fundamentalmente en la esfera del entonces Ministerio de Modernización, aprovechando, reorganizando y expandiendo la infraestructura TIC que ya se venía desarrollando de años anteriores (Datacenter ARSAT; despliegue de fibra óptica, 4G y terminales satelitales VSAT)

[30] Decreto 434/2016 – (01/03/2016)

- Gobierno Abierto e Innovación Pública: Implementación de una plataforma horizontal informática de generación de documentos y expedientes electrónicos, registros y otros contenedores que sea utilizada por toda la administración a los fines de facilitar la gestión documental, el acceso y la perdurabilidad de la información, la reducción de los plazos en las tramitaciones y el seguimiento público de cada expediente.

  Las principales actividades al respecto fueron:

  - Implementación de una plataforma de gestión documental de expedientes y documentos electrónicos, y otros contenedores en todo el sector público.
  - Implementación una plataforma de tramitación a distancia con el ciudadano sobre los sistemas de gestión documental y expediente electrónico.
  - Implementación de acciones para la generación de reportes de datos con el objetivo de contar con información estadística.
  - Desarrollo, mejora continua e integración de los sistemas de gestión.
  - Incorporación de nuevos sistemas y aprovechamiento de iniciativas ya desarrolladas e implementadas que permitan encontrar soluciones transversales de administración integradas al Sistema de Gestión Documental y Expediente Electrónico, procurando cambiar el modelo de desarrollo sectorial, hacia uno homogéneo y cohesionado.
  - Implementación de trámites a distancia y servicios digitales
  - Facilitación a los usuarios para acceder a la plataforma digital de información y servicios administrativos, ampliando los medios de vinculación existentes y facilitando la gestión de trámites a distancia.

  En este campo, es donde se observaron los mayores progresos, ya que no solamente fue una fecunda actividad en el despliegue de infraestructura y recursos humanos; sino que implicó una profunda modernización desde plano normativo, eliminando obstáculos y barreras legales y administrativas que hicieron inviables muchas de las iniciativas impulsadas en gestiones previas.

Universidad de SanAndrés

Sistema de gestión documental electrónica[31]

La ley de firma digital estableció el valor jurídico del documento electrónico, la firma electrónica y la firma digital, y en la disposición, se promovió el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a una progresiva despapelización de la administración pública nacional.

En este sentido, se aprobó la implementación del sistema de Gestión Documental Electrónica —GDE— como sistema integrado de caratulación, numeración, seguimiento y registración de movimientos de todas las actuaciones y expedientes del Sector Público Nacional, sirviendo el sistema como plataforma para la implementación de gestión de expedientes electrónicos; definiendo la autoridad de aplicación del sistema y sus competencias. Asimismo se establecieron las funciones de los administradores locales en cada organismo del Estado y otras medidas administrativas y de coordinación.

Este sistema está integrado por varios módulos, entre los que destacamos:

31 Decreto 561/2016 - (06/04/2016)

- **Escritorio Único (EU):** Navegador para acceder a todos los módulos que integran el sistema.
- **Comunicaciones Oficiales (CCOO):** permite la generación, registro y archivo de documentos comunicables.
- **Generador Electrónico de Documentos Oficiales (GEDO):** permite generar, firmar, registrar y archivar todos los documentos oficiales electrónicos.
- **Expediente Electrónico (EE):** permite la caratulación, vinculación de documentos, pases y consultas de expedientes electrónicos.
- **Registros Legajo Multipropósito (RLM):** permite administrar los documentos respaldatorios de los diversos registros públicos en forma electrónica, con el objeto de identificar personas físicas, jurídicas o cosas y habilitarlas a realizar actividades.
- **Porta firma (PF):** permite administrar la firma de los documentos electrónicos. Brinda la posibilidad de firmar varios documentos al mismo tiempo y de filtrar por lotes los documentos a firmar. Funciona como una bandeja de firmas virtual.
- **Repositorio Único de Documentos Oficiales (RUDO):** permite el guardado y consulta de todos los documentos brindando interoperabilidad entre todas las aplicaciones del Gobierno, pues todos los documentos tienen el mismo formato y residen en un solo repositorio.
- **Trámites a distancia (TAD):** permite a los ciudadanos realizar trámites ante la Administración Pública Nacional durante las 24hs. desde cualquier dispositivo con internet sin tener que acudir a una oficina pública.
- **Interoperar**: Plataforma (Enterprise Service Bus) para interoperación restantes módulos.

Todos los módulos fueron progresivamente implementados con éxito en el organismo que nos ocupa (Prefectura Naval Argentina – Registro Nacional de Buques).

Más allá de lo instrumental en cuanto al significativo esfuerzo que ocasionó la adopción de la gestión electrónica de documentos, como indicamos más arriba, se adoptaron una serie de modificaciones normativas que allanaron su implementación.

Trámites a distancia (TAD)[32]

Se impulsaron distintas medidas tendientes a facilitar la relación de ciudadanos a los organismos del Estado, agilizando sus trámites administrativos, incrementando la transparencia y accesibilidad, mediante el uso una Plataforma de Trámites a Distancia (TAD) como herramienta de acceso, presentación de documentación, seguimiento de trámites y notificaciones en el Sistema de Gestión Documental Electrónica - GDE por parte de los administrados.

A los fines de dar certeza jurídica al trámite electrónico, se estableció la validez de las notificaciones electrónicas realizadas en la plataforma “Trámites a Distancia” (TAD), así como la constitución del domicilio especial electrónico constituido en la cuenta de usuario de dicha plataforma, garantizando la validez jurídica, confidencialidad, seguridad e integridad de la información notificada

Se estableció que la fecha cierta de presentación de escritos por los particulares y de elaboración de los actos administrativos cuando se realicen a través de la plataforma de “Trámites a Distancia” (TAD) y del sistema de Gestión Documental Electrónica (GDE); permitiendo la firma digital de las actuaciones administrativas, mediante dispositivos criptográficos para el caso de los actos administrativos, y certificados de aplicaciones para todas las demás actuaciones (de mero trámite), brindando un marco de seguridad y confianza tecnológica y jurídica a los documentos electrónicos.

[32] - Decreto 1063/2016 (04/10/2016)

Se dispuso la digitalización de la documentación, por lo que la presentación de documentos en la plataforma debe realizarse en formato electrónico; y a tal fin, los usuarios pueden solicitar la digitalización de los documentos que deban presentar y que conste en soporte papel en la sede del organismo pertinente.

El sistema de Gestión Documental Electrónica (GDE) deja constancia de la fecha y hora de presentación de los escritos realizada por los particulares en la Plataforma de "Trámites a Distancia" (TAD) y de los actos producidos por los usuarios de dicho sistema.

Establece que el sistema de Gestión Documental Electrónica (GDE) permite la firma digital de los documentos electrónicos en los siguientes casos:

- Para firmar actos administrativos mediante firma digital con dispositivo criptográfico.
- Para firmar todos los demás actos que no constituyan actos administrativos mediante firma digital con certificado del sistema.

Indica que ambas firmas digitales gozan de plena validez en virtud de lo dispuesto en el artículo 9° de la Ley N° 25.506, asegurando indubitablemente la autoría e integridad del documento electrónico firmado digitalmente.

Buenas Prácticas en Materia de Simplificación [33]

A fin de contribuir al plan de modernización, reducir las cargas sobre los administrados, disminuir los requisitos para suministrar información y datos y evitar la presentación de documentación que el administrado haya aportado, exhibido y/o informado con anterioridad en algún organismo del Sector Público Nacional, utilizando para ello los medios electrónicos y digitales que se encuentran disponibles, se aprobaron Buenas Prácticas en Materia de Simplificación aplicables para el funcionamiento del Sector Público Nacional, que se resumen en los siguientes puntos:

- Simplificación normativa. Las normas y regulaciones que se dicten deberán ser simples, claras, precisas y de fácil comprensión. El Sector Público Nacional deberá confeccionar textos actualizados de sus normas regulatorias y de las guías de los trámites a su cargo. Deberá evaluarse su inventario normativo eliminando las que resulten una carga innecesaria. En el mismo sentido el dictado de nuevas regulaciones que impongan cargas deberán a su vez reducir el inventario existente.
- Mejora continua de procesos. El Sector Público Nacional deberá aplicar mejoras continuas de procesos, a través de la utilización de las nuevas tecnologías y herramientas informáticas, utilizar e identificar los mejores instrumentos, los más innovadores y los menos onerosos, con el fin de agilizar procedimientos administrativos, reducir tiempos que afectan a los administrados y eliminar regulaciones cuya aplicación genere costos innecesarios.
- Evaluación de la implementación. Todos los organismos del Sector Público Nacional deberán tender, en los casos que corresponda, a la evaluación de la implementación de las normas regulatorias que dicten.
- Participación ciudadana. Los organismos del Sector Público Nacional incrementarán los mecanismos de participación, intercambio de ideas, consulta, colaboración y de cultura democrática, incorporando las nuevas tecnologías, necesarios para facilitar la comprensión y medir el impacto que traerá aparejado las nuevas regulaciones.
- Presunción de buena fe. Las regulaciones que se dicten deben partir del principio que reconoce la buena fe del ciudadano, permitiéndole justificar a través de declaraciones juradas situaciones fácticas que deban acreditarse ante los organismos del Sector Público Nacional.

[33] Decreto 891/2017 (01/11/2017)

- Gobierno digital. El Gobierno Nacional deberá fomentar la interoperabilidad entre las administraciones públicas provinciales, y de la Ciudad Autónoma de Buenos Aires, generando de esta manera un intercambio y colaboración mutua, a fin de implementar todas las herramientas tecnológicas existentes, permitiendo de este modo acercar a los ciudadanos herramientas eficaces para su interacción con la Administración.
- Medición de costo-beneficio. El diseño de las regulaciones procurará la incorporación de la medición de los costos-beneficios que impliquen su implementación.
- Silencio positivo. En la elaboración de las normas regulatorias deberá tenerse en cuenta la posibilidad de incrementar el carácter positivo del silencio de la Administración, en la medida que resulte posible en atención a la naturaleza de las relaciones jurídicas tuteladas por la norma de aplicación, siempre y cuando sea en beneficio del requirente y no se afecten derechos a terceros.
- Comunicación eficiente. Los organismos del Sector Público Nacional deberán promover el intercambio de buenas prácticas comunicacionales intra y extra organismos. La totalidad de las medidas dispuestas deberán comunicarse de manera clara y eficiente.
- Creación de registros. En caso de crearse nuevos Registros, en el ámbito de la administración centralizada se requerirá la previa autorización del Jefe de Gabinete de Ministros, mientras que en los demás casos dicha autorización será otorgada por el Poder Ejecutivo Nacional. Los nuevos Registros que se creen deberán ser digitales, facilitando el acceso por parte de los ciudadanos y estarán regidos por el principio de gratuidad.

En particular adquieren gran relevancia las siguientes: “presunción de buna fe” y “silencio positivo”.

En el primer caso, en los hechos, facilita que la persona no tenga que concurrir con el documento a una repartición oficial; basta que adjunte una imagen digital del documento al expediente electrónico y por imperio de la “presunción de buena fe” se impide al funcionario – salvo que exista una duda razonable– solicite el documento original al ciudadano para comprobar su legitimidad.

En cuanto al “silencio positivo”; previamente la administración disponía de 90 días hables para contestar un expediente. En caso de no hacerlo, debía recurrirse al instituto del “pronto despacho” y después de otros 30 días más, se podía interpretar silencio de la administración, habilitando la vía judicial para reclamar. Si bien se legisla en abstracto, da una precisa idea de cuál deben ser los tiempos y la conducta que debe observar el funcionario para resolver las cuestiones administrativas.

Reglamento de Procedimientos Administrativos[34]

En virtud de las discrepancias que surgieron entre el texto vigente en este reglamento y las sucesivas normas que el PEN emitió a raíz del proceso de modernización del Estado, se hizo evidente la necesidad de actualizar la normativa vigente para asimilar en su texto la nueva normativa.

Destacamos entonces, y siempre sin perder de vista el alcance de nuestro trabajo, los siguientes conceptos que marcan los principios de la nueva gestión electrónica de la administración pública:

- Los expedientes administrativos tramitarán por medios electrónicos y serán resueltos con intervención del órgano al que una ley o un decreto hubieren atribuido competencia; …
- Se utilizará el Sistema de Gestión Documental Electrónica y tramitarán los asuntos mediante expedientes electrónicos.

El Órgano competente dirigirá el procedimiento procurando observar que:

- Los expedientes tendrán formato electrónico y se formarán mediante la agregación ordenada de los documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias que deban integrarlos.
- La tramitación de las actuaciones, comunicaciones, documentos y expedientes se realizará mediante el Sistema de Gestión Documental Electrónica, que permite realizar de manera integral la caratulación, numeración, seguimiento y registro de movimientos de todas las actuaciones y

[34] - Decreto 894/2017 t.o. (01/11/2017).

expedientes del Sector Público Nacional. Dicho sistema actuará como plataforma para la implementación de la gestión de los expedientes electrónicos.

- Todos los documentos que formen parte de un expediente deberán ser generados previamente en forma electrónica, o bien, si existieran en papel u otro formato, deberán ser digitalizados de acuerdo a la normativa vigente.
- Los expedientes electrónicos y los documentos electrónicos serán identificados de manera uniforme para toda la Administración a través del Sistema de Gestión Documental Electrónica.
- Documentos electrónicos adjuntos. Se podrán adjuntar documentos electrónicos como archivos embebidos en otros documentos electrónicos. Los particulares podrán presentar escritos en la mesa de entradas del organismo, en las representaciones Diplomáticas u Oficinas Consulares de la República Argentina en el extranjero cuando fuera procedente o en forma electrónica a través de la plataforma electrónica de Trámites a Distancia (TAD), por sí, o mediante representantes o apoderados.
- Todo documento electrónico firmado digitalmente en el Sistema Electrónico de Gestión Documental tendrá carácter de original, y los reproducidos en soporte electrónico a partir de originales de primera generación en cualquier otro soporte, digitalizados de acuerdo al procedimiento que establezca la normativa aplicable serán considerados originales y tendrán idéntica eficacia y valor probatorio que sus equivalentes en soporte papel.
- Recaudos. Todo escrito por el cual se promueva la iniciación de una gestión ante la Administración Pública Nacional deberá contener los siguientes recaudos:
    - Nombres, apellido, indicación de identidad y domicilio real y constituido del interesado.
    - Firma del interesado o de su representante legal o apoderado.
- La cuenta de usuario de la plataforma electrónica de Trámites a Distancia (TAD) será considerada el domicilio especial electrónico constituido para aquellos trámites que se gestionen utilizando dicha plataforma.
- Sede electrónica. La cuenta de usuario de la Plataforma Electrónica de “Trámites a Distancia” (TAD) es la sede electrónica del particular, en donde serán notificadas en forma electrónica las actuaciones administrativas.
- Domicilio real. El domicilio real de la parte interesada debe ser denunciado en la primera presentación que haga aquélla personalmente o por apoderado o representante legal, tanto a través de la Plataforma Electrónica de “Trámites a Distancia” (TAD) como en soporte papel. En caso contrario —como así también en el supuesto de no denunciarse su cambio— y habiéndose constituido domicilio especial se intimará que se subsane el defecto, bajo apercibimiento de notificar en este último todas las resoluciones, aun las que deban efectuarse en el real.
- Todo escrito inicial o en el que se deduzca un recurso podrá presentarse a través de la plataforma electrónica de Trámites a Distancia (TAD), en la mesa de entradas o receptoría del organismo competente o podrán emitirse por correo. El sistema electrónico dejará constancia de la fecha y hora de presentación de los escritos realizada por los particulares en dicha plataforma electrónica y de los actos producidos por los usuarios de dicho sistema.
- Los escritos posteriores podrán presentarse o remitirse igualmente a la oficina donde se encuentra el expediente, o a través de la plataforma electrónica de Trámites a Distancia (TAD). La autoridad administrativa deberá dejar constancia en cada escrito de la fecha en que fuere presentado, poniendo al efecto el cargo pertinente. En caso de duda deberá estarse a la fecha enunciada en el escrito y en su defecto, se considerará que la presentación se hizo en término. El escrito no presentado dentro del horario administrativo del día en que venciere el plazo, solo podrá ser entregado válidamente, en la oficina que corresponda, el día hábil inmediato y dentro de las dos (2) primeras horas del horario de atención de dicha oficina. En los expedientes electrónicos se aplicarán los plazos establecidos en el artículo 30 inciso b) del reglamento no siendo de aplicación

el artículo 124 del Código Procesal Civil y Comercial de la Nación. (derogado por ley 25.488) Esto es que la carga de documentación puede realizarse durante las veinticuatro (24) horas de todos los días del año. El cómputo de plazos se hará a partir del primer día hábil siguiente al de la carga de documentación efectuada correctamente por el particular en la plataforma electrónica en su cuenta de usuario.

- Firma de los documentos por profesionales. Los documentos y planos que se presenten, excepto los croquis deberán estar firmados por profesionales inscriptos en matricula nacional, provincial o municipal, indistintamente.
- De toda actuación que se inicie en Mesa de Entradas o Receptoría se dará una constancia con la identificación del expediente que se origine. Los interesados que hagan entrega de un documento o escrito podrán, además, pedir verbalmente que se les certifique una copia de los mismos. La autoridad administrativa lo hará así, estableciendo que el interesado ha hecho entrega en la oficina de un documento o escrito bajo manifestación de ser el original de la copia suscripta.
- Forma de las notificaciones. Las habituales y se agrega por medio de la plataforma electrónica de trámites a distancia (TAD), que se realizarán en la cuenta de usuario que es la sede electrónica en la cual el particular ha constituido su domicilio especial electrónico. La notificación oficial se dará como perfeccionada cuando el contenido de la misma esté disponible en la cuenta de usuario de destino. A dichos efectos, se considerará al usuario notificado el primer día hábil siguiente al de la fecha de ingreso de la notificación a su cuenta, momento en el que comienzan a correr los plazos.
- Eliminación de cargas al administrado. En aquellos casos que para la sustanciación de un procedimiento administrativo sea necesaria la presentación de alguna información, dato, documento o certificado que deba ser emitido por otra entidad o jurisdicción del Sector Público Nacional, la entidad responsable del procedimiento lo solicitará directamente por comunicación oficial al organismo responsable de su producción y certificación. La solicitud del dato, información, documentación o certificado deberá expresar el motivo, el procedimiento en el cual se enmarca, y la norma que justifica su presentación.
- Presentación de datos y documentos. Los interesados que interactúen con la Administración deberán aportar al procedimiento administrativo los datos y documentos exigidos de acuerdo con lo dispuesto en la normativa aplicable. Asimismo, podrán aportar cualquier otro documento que estimen conveniente. La Administración no exigirá a los interesados la entrega de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.
- A los efectos del Reglamento, se entenderá por Declaración Jurada:
    - El documento suscrito por un interesado en el que éste manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para obtener el reconocimiento de un derecho o facultad para su ejercicio, que dispone de la documentación que así lo acredita, que la pondrá a disposición de la Administración cuando le sea requerida, y que se compromete a mantener el cumplimiento de las anteriores obligaciones durante el período de tiempo inherente a dicho reconocimiento o ejercicio. Los requisitos a los que se refiere el párrafo anterior deberán estar recogidos de manera expresa, clara y precisa en la correspondiente Declaración Jurada. La Administración podrá requerir en cualquier momento que se aporte la documentación que acredite el cumplimiento de los mencionados requisitos y el interesado deberá aportarla.
    - El documento mediante el que los interesados ponen en conocimiento de la Administración sus datos identificatorios o cualquier otro dato o documentación relevante para el inicio de una actividad o el ejercicio de un derecho.

  La inexactitud, falsedad u omisión, de carácter esencial, de cualquier dato o información que se incorpore a una Declaración Jurada o la no presentación ante la Administración de la documentación que sea en su caso requerida para acreditar el cumplimiento de lo declarado,

podrá generar una sanción, sin perjuicio de las responsabilidades penales, civiles o administrativas a que hubiera lugar. Asimismo, la resolución de la Administración Pública que declare tales circunstancias podrá determinar la obligación del interesado de restituir la situación jurídica al momento previo al reconocimiento o al ejercicio del derecho o al inicio de la actividad correspondiente, todo ello conforme a los términos establecidos en las normas de aplicación.

Simplificación y desburocratización de la Administración Pública Nacional[35]

Mediante la Ley 27446, se amplía la eficacia de la firma digital al eliminar las exclusiones que marcaba el Art, 4 la ley de firma digital; se corrige la redacción respecto al presunción (Art.10) indicando que cuando un documento electrónico sea firmado por un certificado de aplicación, se presumirá, salvo prueba en contrario, que el documento firmado proviene de la persona titular del certificado y se establece que los documentos oficiales electrónicos firmados digitalmente, expedientes electrónicos, comunicaciones oficiales, notificaciones electrónicas y domicilio especial constituido electrónico de la plataforma de trámites a distancia y de los sistemas de gestión documental electrónica que utilizan el sector público nacional, las provincias, el gobierno de la Ciudad Autónoma de Buenos Aires, municipios, poderes judiciales, entes públicos no estatales, sociedades del Estado, entes tripartitos, entes binacionales, Banco Central de la República Argentina, en procedimientos administrativos y procesos judiciales, tienen para el sector público nacional idéntica eficacia y valor probatorio que sus equivalentes en soporte papel o cualquier otro soporte que se utilice, debido a la interoperabilidad producto del reconocimiento automático en los sistemas de gestión documental electrónica, por lo que no se requerirá su legalización.

Por otra parte, señala que las jurisdicciones y entidades contempladas de la administración pública nacional, formularán, suscribirán y remitirán las respuestas a los oficios judiciales exclusivamente mediante el Sistema de Gestión Documental Electrónica –GDE–.

Universidad de SanAndrés

[35] Ley 27446 – 30/06/2018

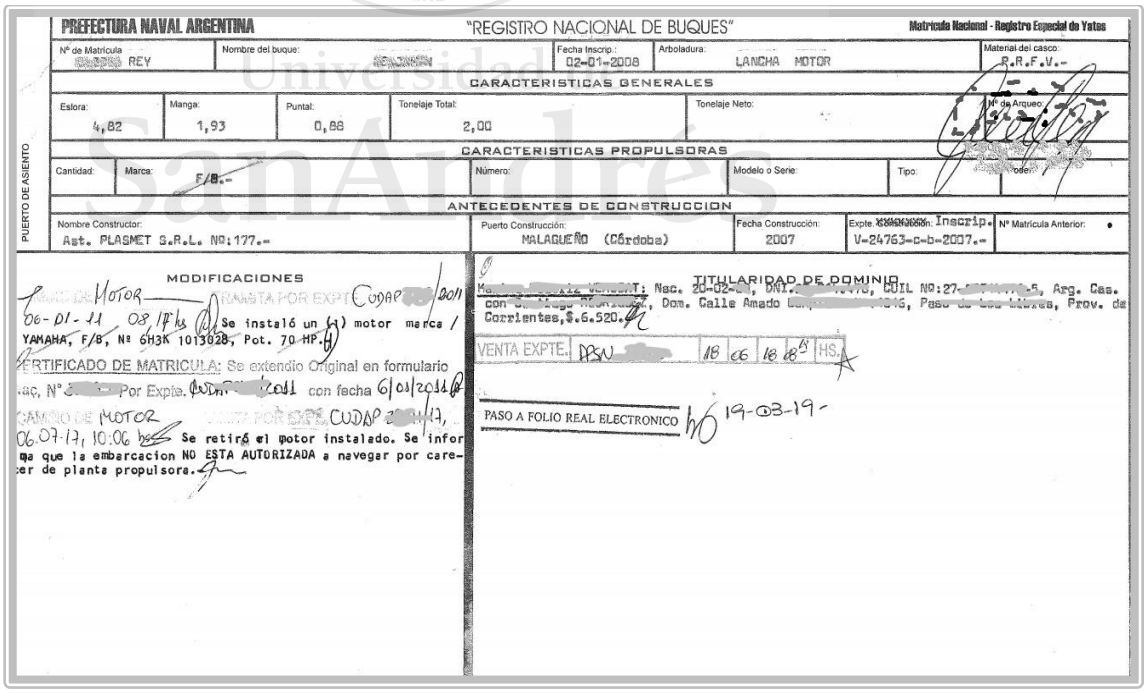
Capítulo 4 – El sistema vigente

Estado inicial

La gestión del Registro Nacional de Buques, previo a su proceso de modernización, poseía las siguientes características:

- Trámites basados en soporte papel, mayoritariamente iniciados a partir de 'formulario tipo' completado y firmado por el usuario o su representante legal, más la pertinente documentación respaldatoria agregada; todo lo cual se presenta en mesa de entrada del propio registro o en una dependencia jurisdiccional del organismo, conformando un expediente que se deriva al área correspondiente del registro para su resolución. Los asientos registrales que correspondan se vuelcan con máquinas de escribir, en el 'folio real' de tipo 'cartular', fichas de cartón de 25 x35 cm de diferentes colores según la agrupación.
- El escribano actuante, con el expediente en soporte papel y folio real a la vista, controla el trámite y de proceder, firma en forma manuscrita el correspondiente registro.
- Existe un sistema informático para consulta de las características principales de los buques y sus propietarios, denominado Sistema Integrado de Buques (SIB). Este sistema permite al acceso a distintas bases de datos disponibles en Prefectura; sin embargo para el personal del Registro resulta en general poco confiable, debido a que posee datos incompletos, erróneos, desactualizados y/o inconsistentes.
- El escribano antes de actuar, recurre al folio real físico, para tenerlo a la vista –única fuente confiable- y así determinar fehacientemente la situación jurídica del buque y proceder en consecuencia. Los expedientes una vez tramitados, se pueden acumular por largos períodos a la espera de disponibilidad de personal y medios, para proceder al volcado de los datos modificados al sistema informático. También es posible encontrar expedientes que hayan seguido su curso, sin que se haya advertido la necesidad de cargar las actualizaciones en el sistema. Esta situación, es responsable en gran medida de la inconsistencia de datos que existe entre lo que se encuentra registrado en folio real y la información que está disponible en el sistema.
- Analizando esta problemática, se infiere que la actualización de datos en el sistema informático es percibida por parte del personal del Registro como una tarea secundaria, gravosa y que puede ser diferida en el tiempo. Cuando vemos la mecánica del proceso, advertimos que los escribanos consienten ser los responsables primarios de los asientos en el folio real, los cuales fechan y certifican con su firma ológrafa; en cambio no se hacen cargo por la exactitud ni oportunidad en que la información es volcada al sistema.
- En cuanto al software del sistema informático existente, carece de las interfaces adecuadas para poder ser usado con seguridad en entorno web. Carece de una interfaz para llenado de formularios, en consecuencia no existe la posibilidad de recuperar información del sistema para validar los datos de entrada o pre-elaborar automáticamente los asientos registrales o documentos que surgen del trámite. Esto obliga a transcribir los formularios, lo que demanda tiempo y genera doble trabajo, con el riesgo que los datos volcados al sistema difieran de los originalmente consignados en el papel.

- La tecnología e interfaz gráfica de usuario del aplicativo es tecnológicamente obsoleta, carece de un framework[36] para documentar y gestionar el flujo de los procesos, en tanto el diseño de la base de datos resulta deficiente.
- Otros departamentos de la organización administran sistemas que también involucran la gestión documental y técnica del buque, sin embargo no están integrados y los datos no están disponibles en una base de datos común para todo el organismo (silos departamentales).
- El registro de medidas judiciales se realiza mediante anotación en libros índices, denominados "libro verde" para inhibiciones sobre las personas y "libro azul" para registrar medidas sobre buques (previo a su inscripción en el folio). En forma diferida y cuando se cuenta con personal y medios disponibles, se vuelcan estas inhibiciones y medidas en un sistema informático fuera de línea, residente en una PC, sin mantenimiento y desactualizado. La falta de sincronización entre estas tareas, provoca que para determinar si un buque o personas poseen restricciones se deba: consultar el correspondiente libro índice; consultar el sistema y adicionalmente la bandeja de entrada de expedientes aún no registrados.
- La liquidación de aranceles por los trámites se realiza mediante un sistema centralizado de liquidación y cobro a través de plataformas electrónicas (ATFA – Aranceles y Tasa Fija Anual), sin que exista interoperatibilidad con el sistema SIB.
- No se dispone de un sistema de gestión de documentos y expedientes en trámite en el Registro, haciendo imposible conocer en cualquier momento el tipo, cantidad, ubicación y estado de los trámites en curso. Tampoco se pueden obtener o implantar métricas o indicadores claves de gestión para evaluar el rendimiento de los procesos y adoptar las correcciones o mejoras necesarias para mitigar los cuellos de botella.


PREFECTURA NAVAL ARGENTINA — "REGISTRO NACIONAL DE BUQUES" — Matrícula Nacional - Registro Especial de Yates

Nº de Matrícula: REY | Nombre del buque: | Fecha Inscrip.: 02-01-2008 | Arboladura: LANCHA MOTOR | Material del casco: R.R.F.V.-

CARACTERISTICAS GENERALES

Eslora: 4,82 | Manga: 1,93 | Puntal: 0,88 | Tonelaje Total: 2,00 | Tonelaje Neto: | Nº de Arqueo:

CARACTERISTICAS PROPULSORAS

Cantidad: | Marca: F/B.- | Número: | Modelo o Serie: | Tipo: | Poder:

ANTECEDENTES DE CONSTRUCCION

Nombre Constructor: Ast. PLASMET S.R.L. Nº:177.- | Puerto Construcción: MALAGUEÑO (Córdoba) | Fecha Construcción: 2007 | Expte. [redacted]: Inscrip. V-24763-c-b-2007.- | Nº Matrícula Anterior:

PUERTO DE ASIENTO

MODIFICACIONES

CAMBIO DE MOTOR — HABILITADA POR EXPTE CUDAP [redacted]/2011

06-01-11 08 HS Se instaló un (1) motor marca / YAMAHA, F/B, Nº 6H3K 1013028, Pot. 70 HP.-

CERTIFICADO DE MATRICULA: Se extendio Original en formulario [illegible] Nº [redacted] Por Expte. CUDAP [redacted]/2011 con fecha 6/01/2011

CAMBIO DE MOTOR — HABILITADA POR EXPTE CUDAP [redacted]/17,

06-07-17, 10:06 hs Se retiró el motor instalado. Se informa que la embarcacion NO ESTA AUTORIZADA a navegar por carecer de planta propulsora.-

TITULARIDAD DE DOMINIO

[redacted] Nac. 26-02-[redacted], DNI [redacted], CUIL Nº:27-[redacted]-5, Arg. Cas. con [redacted], Dom. Calle Amado [redacted], Paso de los Libres, Prov. de Corrientes, $.6.520.-

VENTA EXPTE. DPSU [redacted] 18 06 18 18 HS.

PASO A FOLIO REAL ELECTRONICO 19-03-19-

Ilustración 19 - Folio Real Cartular (FRC)

[36] Estructura tecnológica de asistencia, con módulos concretos de *software*, que sirven para la organización y desarrollo de software., con soporte de programas, bibliotecas y un lenguaje interpretado, que ayudan al desarrollo y consistencia de los diferentes componentes de un sistema.

Estado actual

Como consecuencia de las características apuntadas en el punto anterior, se ejecutó un proceso de modernización y transformación administrativa interna en el organismo, en el que se procedió básicamente a:

Implementación de un nuevo sistema de gestión (PROGEBU)

- Se efectuó una reingeniería y se procedió a desarrollar un nuevo sistema informático de gestión, (PROGEBU – Proceso de Gestión del Buque) basado en una herramienta de modelado de procesos (Oracle BPM) e interfaces generadas en un framework de desarrollo de aplicaciones estándar (Oracle ADF). La explotación de los datos se hace mediante una herramienta de businesses intelligent (Oracle BI) lo que permite la extracción de información estadística a partir de los datos y su uso en la operación diaria o para el análisis para facilitar la toma de decisiones. De este modo se procede a normalizar, documentar y abordar el flujo de los trámites de manera integrada, privilegiando el flujo horizontal de la gestión por sobre las verticales departamentales. Se dispuso la carga de datos del formulario directamente en el punto de atención al público, dando inicio allí a la gestión del proceso del trámite.
- Se desarrolló un nuevo sistema para registrar y consultar los expedientes referidos a medidas cautelares sobre buques e inhibiciones sobre las personas (PROGEBYP). En el caso que la medida corresponda ser registrada en el folio real, se deriva automáticamente la tarea al PROGEBU. Previo a poner en producción este sistema, se migraron y normalizaron todos los datos existentes en el anterior, como así también se hizo el vuelco de la información contenida en los libros índice, facilitando así que las consultas se puedan realizar de manera electrónica, prescindiendo de los registros manuales en los libros.
- Se estableció un nuevo formulario para el folio real, adoptando el modelo denominado “folio real electrónico” (FRE). De este folio se genera una nueva versión en cada oportunidad que se incorporan asientos y se firma electrónicamente por el escribano interviniente. Los registros que son autogenerados por el sistema en base al tipo de trámite y datos precargados desde el sistema, con lo que se logra reducir la intervención operadores del registro, mejorando la precisión, velocidad y consistencia de datos.
- Se centralizaron las bases de datos existentes en el organismo, de modo que todas las áreas dispongan de idéntica información; migrándose los datos existentes y clausurando sistemas satélites basados en planillas de cálculos o similar.
- Se cargaron todos los trámites en curso en el nuevo sistema, teniendo ahora la trazabilidad de los expedientes mediante la herramienta de BPM, lo que permite determinar el grado de avance de cada trámite (proceso, estado y tarea en que se encuentra y responsable).
- Se generaron tableros de control e indicadores claves (KPIs) para evaluar el nivel de desempeño de los operadores y el grado de cumplimiento de los objetivos fijados.
- El sistema brinda el estado registral del buque conforme los asientos efectivamente incorporados en el folio real (definitivo) y además permite conocer el ‘estado transaccional´, es decir un estadio intermedio que sucede cuando se está tramitando un cambio. Esto facilita que las autoridades del organismo conozcan la situación real de una embarcación desde el inicio de cualquier expediente, aun cuando no se haya terminado de perfeccionar el trámite.

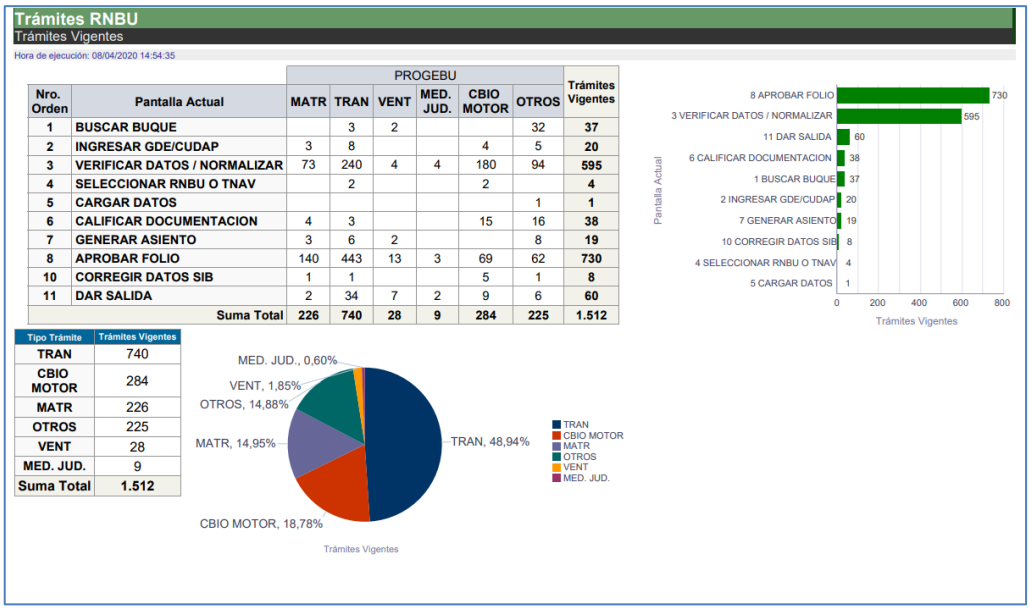


Ilustración 20 - Tablero BI de PROGEBU

Implementación del sistema GDE

En el marco del proceso de modernización del estado, en un trabajo liderado por distintos equipos del entonces ministerio de Modernización, se procedió a la implementación de diferentes módulos disponibles en la plataforma GDE (Gestión Documental Electrónica). Esta plataforma es un sistema de caratulación, numeración, seguimiento y registración de movimientos de todas las actuaciones y expedientes del Sector Público Nacional.

Ilustración 21 - Ecosistema GDE (Ministerio de Modernización, 2018)

Se habilitaron del sistema GDE los siguientes módulos:

A. **Escritorio Único (EU):** Permite ingresar al sistema y navegar por todos los módulos que integran el sistema. El administrador local de la plataforma, habilita los usuarios y se establecen las dependencias orgánicas.

B. **Comunicaciones Oficiales (CCOO):** permite la generación, registro y archivo de documentos comunicables. Documento comunicable, es todo documento oficial que puede ser destinado a uno o varios usuarios internos o externos.

C. **Generador Electrónico de Documentos Oficiales (GEDO):** permite generar, registrar y archivar todos los documentos oficiales electrónicos necesarios para vincular a un expediente electrónico (EE). Los documentos disponibles en GEDO pueden ser:

   - Documentos de redacción libre: son aquellos documentos en los que el usuario redacta todo el contenido a partir de un procesador de textos.
   - Documentos para importar: son aquellos documentos en los que se permite subir un archivo digital con imágenes o generado en otro software a la plataforma, para su certificación a través de una firma electrónica o digital y su resguardo en los servidores del GDE.
   - Documentos con "template" o formularios controlados: son aquellos documentos cuyos campos de redacción o ingreso de datos están preestablecidos.
   - Documentos con archivos embebidos: son documentos que contienen archivos en su extensión original otorgándoles validez tanto al documento como su adjunto.

D. **Expediente Electrónico (EE):** permite la caratulación, vinculación de documentos, pases y consultas de expedientes electrónicos.

E. **Registros Legajo Multipropósito (RLM):** permite administrar los documentos respaldatorios de los diversos registros públicos en forma electrónica, con el objeto de identificar personas físicas, jurídicas o cosas y habilitarlas a realizar actividades.

F. **Porta firma (PF):** permite administrar la firma de los documentos electrónicos. Brinda la posibilidad de firmar varios documentos al mismo tiempo y de filtrar por lotes los documentos a firmar. Funciona como una bandeja de firmas virtual.

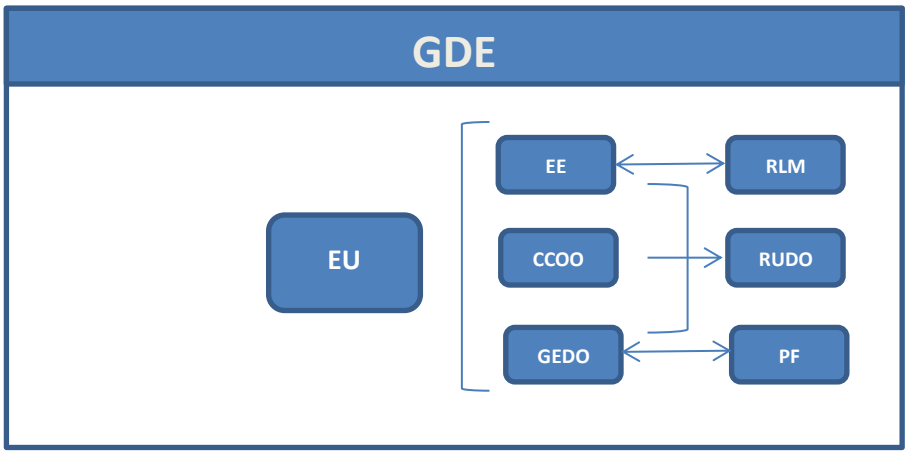
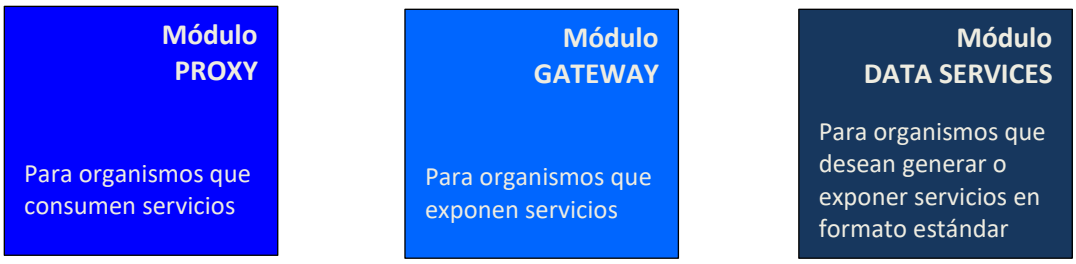


Ilustración 22 - Módulos GDE implementados (Elaboración propia)

G. **Repositorio Único de Documentos Oficiales (RUDO):** permite el guardado y consulta de todos los documentos brindando interoperabilidad entre todas las aplicaciones del Gobierno, pues todos los documentos tienen el mismo formato y residen en un solo repositorio

H. **Interoperar:** es una arquitectura que permite la interoperabilidad de información de manera estándar y segura entre nodos. Posee tres módulos conforme los estándares para intercambio de datos entre organismos:



- El módulo **Data Services** permite crear y exponer servicios web basados en tecnologías **REST** a partir de diferentes fuentes de datos, como base de datos, de una forma fácil, rápida e intuitiva.
- El módulo **Proxy / Consumidor** permite consumir servicios de manera segura mediante el uso de protocolos **HTTPS** y tokens **JWT**, monitoreando y auditando el uso de los mismos.
- El módulo **Gateway / Productor** permite exponer servicios de manera segura mediante el uso de protocolos **HTTPS** y tokens **JWT**, monitoreando y auditando el uso de los mismos.

- **Plataforma de Autenticación Electrónica Central (PAEC)**: La función de PAEC es lograr la autenticación de un usuario, es decir, asegurar que el usuario es quien dice ser; simplificando la relación entre las Aplicaciones Cliente (AP) y los Proveedores de Identidad (PdI) sin modificar la experiencia del usuario final en el proceso de autenticación de un sistema.

  Por AP, se entiende que es cualquier sistema o aplicación que utiliza los servicios del portal AUTENTICAR[37] para resolver las autenticaciones de sus usuarios. Los PdI son cualquier sistema, servicio o aplicación que brinda los servicios de autenticación de usuarios a través de PAEC.

  El servicio ofrecido por la plataforma es gratuito para todos los usuarios; quienes sí pueden aplicar cargos son los Proveedores de Identidad y cada uno de ellos tendrá sus propios términos y condiciones.

- **eRecauda:** tiene como objetivo permitir al Contribuyente/Deudor, en el marco del gobierno electrónico, que a partir de un Portal único, generar sus propios comprobantes para el pago, con el fin de cumplir sus obligaciones con el Estado, representado en los distintos Ministerios u Organismos que lo componen. Luego de completar una serie de datos correspondientes al concepto de pago, el contribuyente podrá optar por la generación de un Volante Electrónico de Pago (VEP), para posteriormente ser pagado en forma electrónica a través de una determinada entidad de pago (Red Banelco, Red LINK, o Interbanking), o por la generación e impresión de una Boleta de Pago, para realizar el mismo en una entidad bancaria o no bancaria adherida al Sistema, en forma presencial.

[37] https://www.argentina.gob.ar/jefatura/innovacion-publica/administrativa/autenticar

Eliminación del soporte papel

Con la implementación del GDE a partir de Octubre de 2018, se inició el proceso de "despapelización" de los expedientes del Registro, ya que los formulario de los trámites pasaron a ser completados via web en los puntos de atención al público (agencias) y junto con los documentos respaldatorios escaneados, subidos a la plataforma GDE donde se genera el expediente electrónico (EE).

Como se advierte en el cursograma "Trámite modelo actual sin TAD", cuando el usuario llega al punto de atención al público, presenta el formulario conforme el trámite que desea efectuar y la documentación respaldatoria de rigor (factura, contrato, documento personal, cuit/cuil, etc.).

En caso de estar completos los requisitos, el operador en la agencia[38] genera un expediente electrónico (EE) en el sistema GDE y un trámite en PROGEBU, los cuales se relacionan internamente. Se escanea la documentación (todo en un solo pdf), que se agrega al EE como un documento gráfico desde GEDO, mientras se archivan los documentos físicos en la dependencia.

Se genera la liquidación de aranceles, pare que el usuario en el sistema eRecauda, proceda a pagar el VEP con medios electrónicos o en caja mediante boleta de pago. El comprobante de pago, se deberá agregar al EE como constancia. En el sistema PROGEBU se completa el formulario del trámite y posteriormente se ejecuta la verificación técnica[39] y se transfiere el trámite al Registro.

En el Registro se "normalizan los datos", proceso que se realiza para asegurarse que la información migrada del antiguo sistema informático SIB al PROGEBU, sea correcta y se corresponda con la obrante en el folio real cartular (FRC) pre-existente, de manera de garantizar en lo sucesivo, la calidad de los datos obrantes en la nueva base de datos (DB).

Paso seguido, se verifica si existen inhibiciones o medidas cautelares que impidan la ejecución de la operación pretendida y luego un oficial de registro efectúa el análisis documental para asegurarse que la documentación se encuentra completa y es válida. Esto habilita la generación de los "asientos" que se transferirán al folio y ocasionarán la actualización de los datos en la DB; los que seguidamente son analizados por el oficial de registro actuante y en caso de ser correcto, procede a "firmar electrónicamente" el "folio real electrónico". Inmediatamente después, se genera el documento o certificado de la operación que se entrega como constancia al usuario a través de la correspondiente agencia, finalizando así el trámite.

Este proceso tuvo gran suceso debido a que contribuyó en mucho a la organización administrativa del Registro, ya que facilitó la disposición y acceso a los expedientes, a la vez que disminuyó el tiempo de tramitación al eliminarse los tiempos muertos propios del correo que existían cuando se enviaban los expedientes papel.

En esta instancia, ya no se permiten más los pagos por ventanilla en la agencia, y es el propio usuario quién en base a la liquidación, procede al pago del arancel por medios electrónicos o por banco en ventanilla. Sin embargo el trámite del expediente no se interrumpe y continúa procesándose hasta la tarea de "generación de asientos", que es cuando se verifica la existencia del comprobante de pago para poder continuar con la tramitación del expediente.

[38] Entiéndase cada sede jurisdiccional del organismo.

[39] Acta de verificación de características.

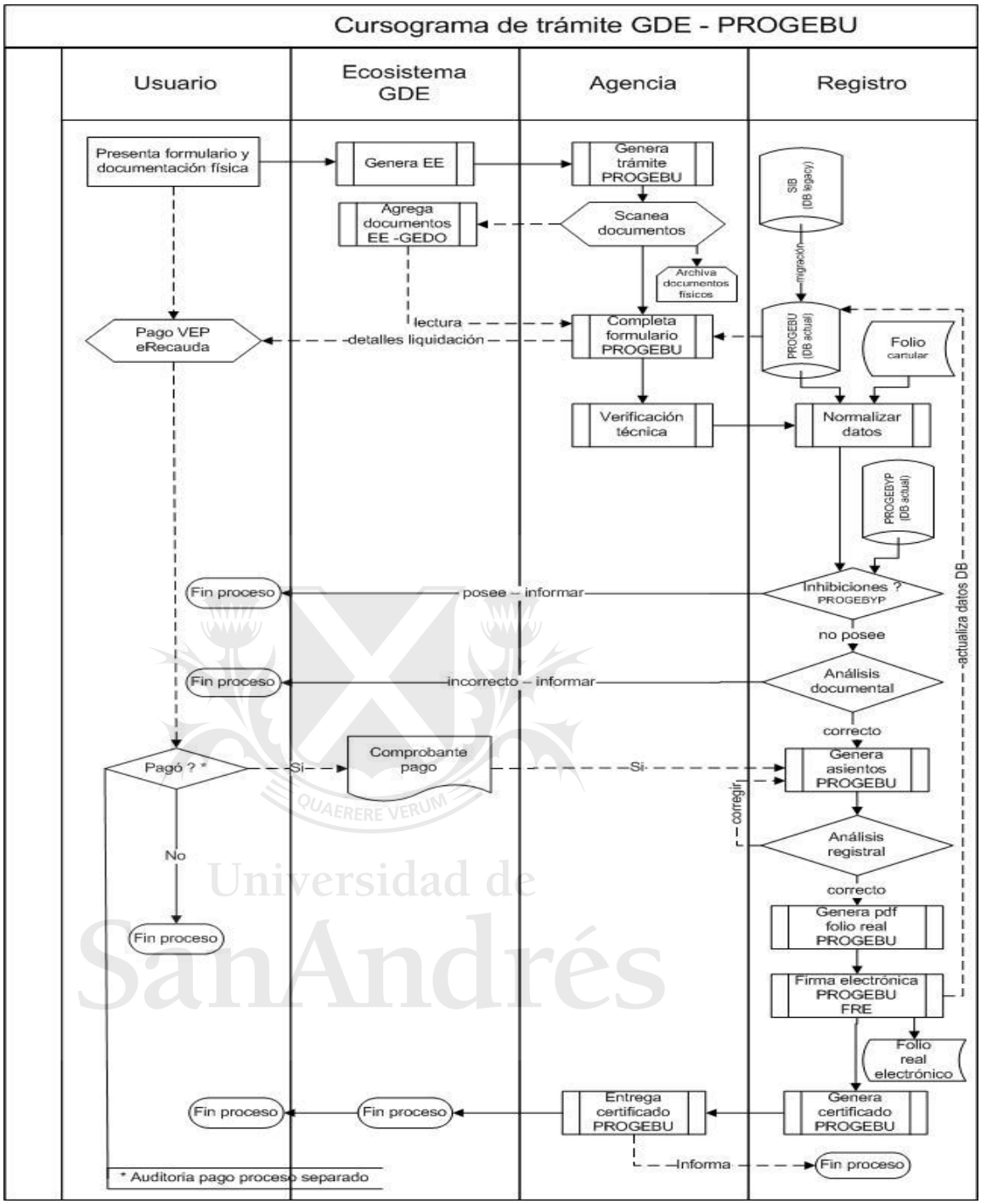


Ilustración 23 - Trámite modelo actual sin TAD[40] (Elaboración propia)

La eliminación del soporte papel, provocó que los operadores tuvieran que adaptarse a usar doble ventana en el escritorio de la PC; y el hecho que todos los documentos estuvieran escaneados en un solo archivo (PDF), ayudó en mucho a la agilización de esta tarea.

[40] Elaboración propia

PREFECTURA NAVAL ARGENTINA **FOLIO**

"REGISTRO NACIONAL DE BUQUES"

DATOS TÉCNICOS

NRO MATRÍCULA: **REY**
NOMBRE DEL BUQUE:
NRO OMI: .-
MATERIAL CASCO: PRFV
FECHA DE INSCRIPCION: 16/ /2020
ARBOLADURA: LANCHA DE MOTOR
EXPTE DE INSCRIPCIÓN: T6
MARCA INDENTIFICACIÓN: AI-07-CUDAP
NOMBRE CONSTRUCTOR: ASTILLERO INDUST-PLAST S.R.L
PUERTO DE CONSTRUCCION: SALADILLO
PUERTO DE ASIENTO: BARADERO

ESLORA (Mts): 5.37
MANGA 1,9
PUNTAL 0.76
ARQUEO BRUTO: 2
ARQUEO NETO: 1
AÑO CONSTRUCCION: 2008
NRO DE UNIDAD: 028
NRO ARQUEO: .-
NRO MATRICULA ANTERIOR: .-

DATOS DEL MOTOR

CANTIDAD DE MOTORES: 1 (Uno) .-
PMA: 50 HP - 37,29 KW

MARCA	NÚMERO	TIPO/COMBUSTIBLE	POTENCIA	MODELO/SERIE
TOHATSU .-	4 B .-	FUERA DE BORDA	40 HP - 29.83 KW	.-

ASIENTOS

TITULARIDAD DOMINIO

NÚMERO	ASIENTO	APROBÓ
1	V , Arg., nac. 22/12/ 5, DNI , soltera, dom. N° , (C.P.) Baradero, Buenos Aires, CUIL: 3-, valor: $,00.-	VE ZQUEZ SILVIA AN RLA

MODIFICACIONES

NÚMERO	ASIENTO	APROBÓ
1	NOTA Por mismo Expte. y fecha de inscrip. se deja constancia C.M.P. 7 (Siete), T.N. COSTERA RESTRINGIDA, C.M. 900 KG, D/N DE PLACER .- CERTIFICADO DE MATRICULA: Se extendió original en formulario Nac. N° y Constancia de Matricula.-	VE ZQUE SILVIA ANDREA

DERECHOS REALES DE GARANTIA - DISFRUTE - ARRENDAMIENTO

****

MEDIDAS CAUTELARES

****

CANCELACIÓN DE DERECHOS REALES DE GARANTIA - DISFRUTE - ARRENDAMIENTO

****

CANCELACIÓN DE MEDIDAS CAUTELARES

Ilustración 24 - Folio Real Electrónico (FRE)

Implementación Trámites a Distancia (TAD)

El portal de Trámites a Distancia[41] (TAD) permite al ciudadano realizar trámites ante la administración pública nacional de manera virtual desde una computadora, durante las 24 h., pudiendo gestionar y realizar el seguimiento de los mismos desde cualquier dispositivo con internet sin la necesidad de tener que acudir a la mesa de entrada de un organismo.

El ingreso a TAD se puede acceder a través de diferentes formas:

- **AFIP: CUIT – Clave Fiscal:** La clave fiscal es una contraseña que otorga la AFIP para realizar trámites (presentar declaraciones juradas, efectuar pagos, adherir al monotributo, solicitar la baja en impuestos o regímenes tributarios, trámites en TAD, etcétera.) desde cualquier PC, tablet o smartphone conectado a internet. Se puede crear un usuario en la plataforma y realizar todos los trámites del sector público nacional.
- **Documento Nacional de identidad – DNI:** El Documento Nacional de Identidad de argentina es el documento primario de identificación con que cuenta cada ciudadano argentino y los extranjeros con domicilio en el territorio del país. El DNI en el sector inferior posee un número de trámite y con él se puede crear un usuario en la plataforma y realizar todos los trámites que estén habilitados para ese nivel de seguridad.
- **ANSES – Clave de Seguridad Social:** La clave de la Seguridad Social es una contraseña para ingresar al portal de gestión Mi ANSES y TAD desde donde se pueden realizar trámites y consultas de manera segura sin necesidad de presentarte personalmente en una oficina.
- **MiArgentina:** Con el usuario de MiArgentina se puede acceder de forma fácil y segura a los servicios digitales del Estado y realizar trámites que poseen un nivel bajo de autenticación.

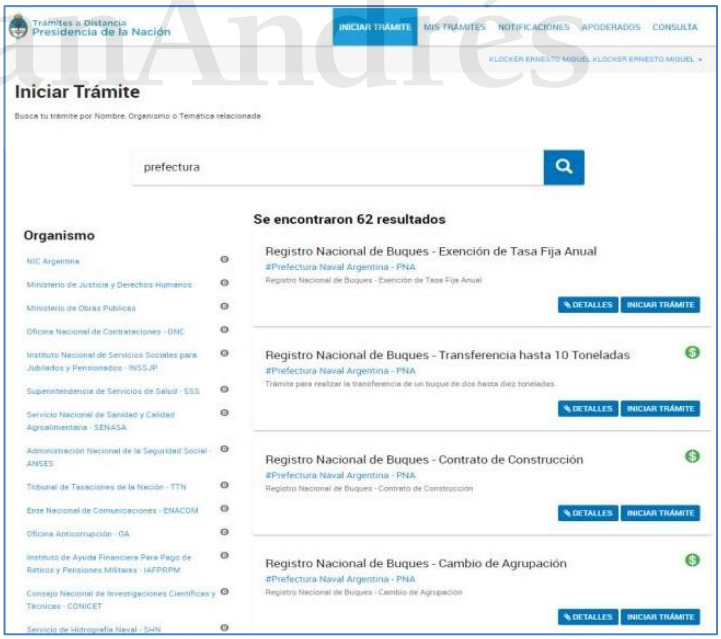


Ilustración 25 - Trámites a distancia (Tramites a distancia, 2020)

[41] https://tramitesadistancia.gob.ar/

En TAD los trámites del Registro Nacional de Buques, se han incorporados a la plataforma el 5 de Noviembre de 2019; son los normales y habituales y la mayoría están arancelado, debiéndo estos pagos ser realizados a través de la plataforma **e-Recauda,** y la conciliación contable del pago fue establecida como una condición necesaria para que se pueda generar el EE en sistema GDE que permite procesar el trámite.

Se indica en cada trámite los documentos que se requieren y se despliegan los campos donde se deben cargar individualmente cada uno.

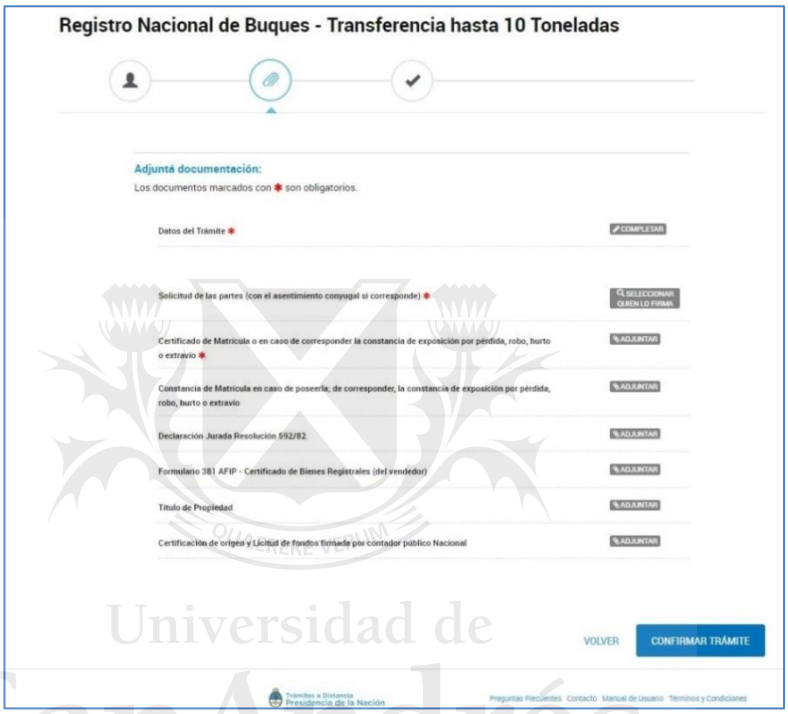


Ilustración 26 - Trámite TAD (Tramites a distancia, 2020)

Esto ocasiona en la práctica que los trámites a distancia se demoren por más de 72 hs hasta que se habilite el EE y se pueda comenzar con generación de la tarea en PROGEBU y gestionar la solicitud.

Algunos datos, vienen pre-cargados, por lo que se requiere verificarlos y en caso de ser necesario modificar los datos incorrectos. Como la plataforma TAD no accede a la base de datos de buques del Registro, para utilizar la información disponible, usa tablas locales que alimentan listas de valores para selección del usuario.

Se deben llenar todos los formularios del trámite y adjuntar los documentos de carácter obligatorio o adicional que se requieren. Por cada formulario o documento agregado se genera un documento que será asociado al expediente electrónico (EE).

Una vez que se ha conciliado el pago y se ha creado el EE, este es derivado a la agencia local, se creará el trámite en PROGEBU y se completará el formulario correspondiente al trámite. El usuario (si corresponde) será notificado que deberá concurrir con la embarcación para que se efectúe la verificación técnica. Paso seguido, se transfiere el trámite al Registro para prosecución.

En el Registro el trámite discurre como en el caso anterior, salvo que en esta ocasión, el folio real una vez generado, se firma digitalmente en el sistema de Gestión Documental (GEDO); se inserta el Folio Real Digital (FRD) en el Registro de Legajo Único (RLM) y en el Repositorio Único (RUDO) del ecosistema GDE.

Universidad de San Andrés

Finalmente, también se envía el certificado del trámite a GEDO, para que éste también sea firmado digitalmente y entregado a través de TAD.

El acceso a los diversos servicios y aplicaciones de GDE, se encuentran segurizados a través de los servicios **JWT GDE Access Token** de la Plataforma de Autenticación Electrónica Central (PAEC) que utiliza el esquema de OAUTH2[42], lo cual implica la utilización de Json Web Token (JWT)[43]. Para acceder a este servicio el usuario previamente debe obtener (en forma transparente) el JWT de PAEC y el JWT "GATEWAY Access Token" de INTEROPERAR.

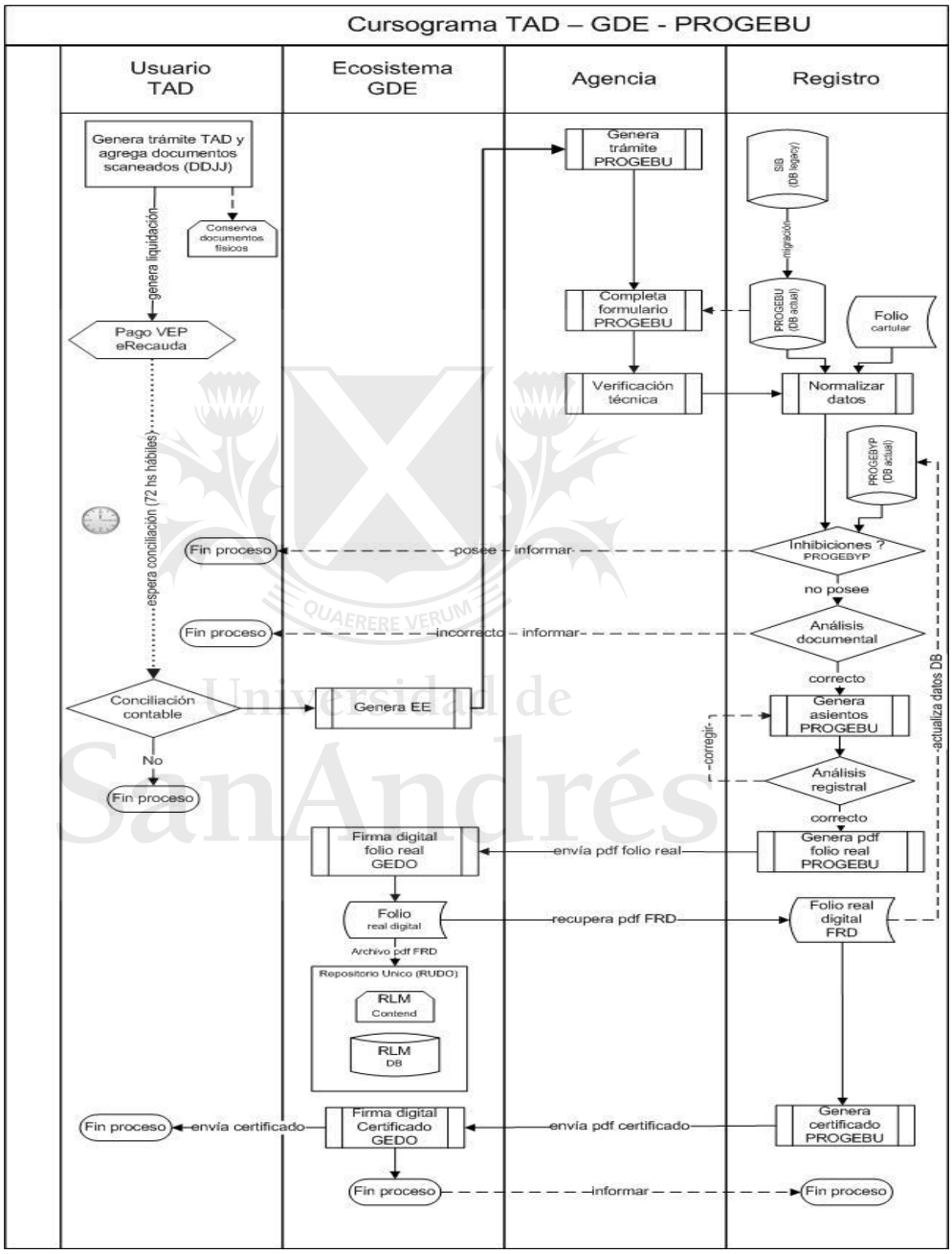


Ilustración 27 - Cursograma de trámite modelo actual con TAD (Elaboración propia)

[42] **OAuth** es un estándar abierto para la delegación de acceso, comúnmente utilizado como una forma para que los usuarios de Internet otorguen a los sitios web o aplicaciones acceso a su información en otros sitios web pero sin darles las contraseñas.(https://en.wikipedia.org/wiki/OAuth)

[43] **JSON Web Token** (**JWT**) es un estándar abierto basado en JSON propuesto por IETF (RFC 7519) para la creación de tokens de acceso que permiten la propagación de identidad y privilegios.(https://es.wikipedia.org/wiki/JSON_Web_Token)

En la siguiente ilustración se observa el Folio Real Digital. El pdf que fue armado en el sistema PROGEBU, se envía al entorno GDE y es importado como un documento del tipo Certificado (más adelante se puede solicitar un tipo de documento específico). En esta condición se firma digitalmente en GEDO, incorporándose las constancias de importación y protocolización del documento.

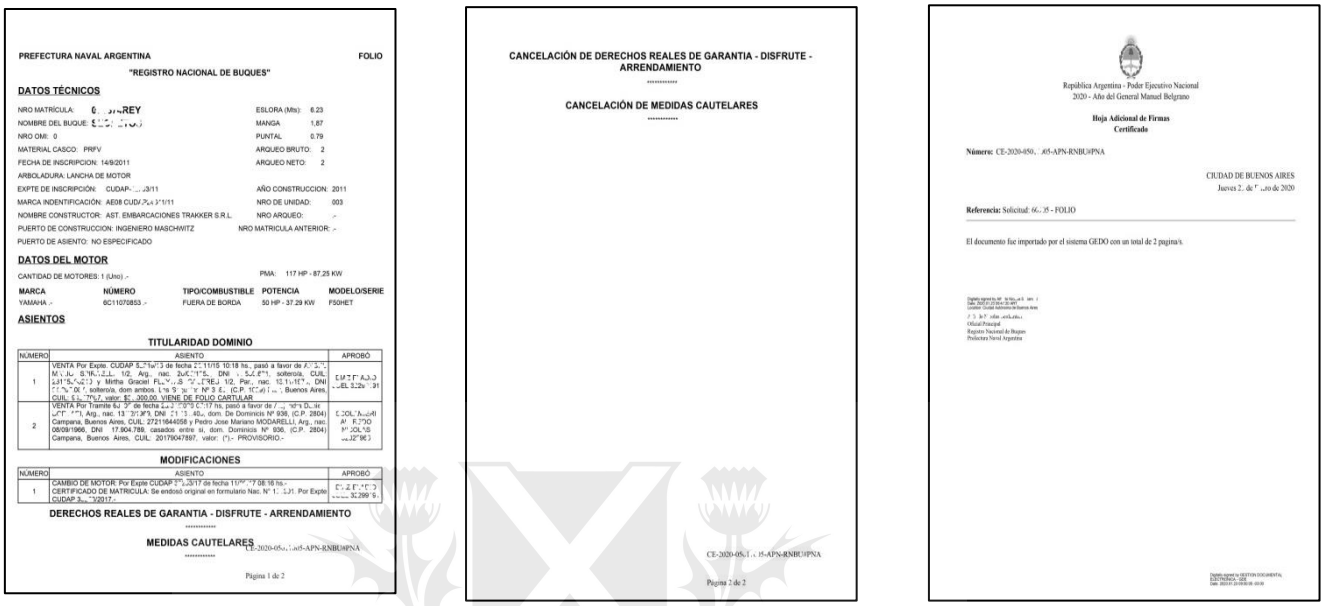


Ilustración 28 - Folio Real Digital (FRD)

Lamentablemente, como se observa en el siguiente tablero, son escasos los trámites que se inician a través de TAD por dificultades técnicas en la implementación de la plataforma; por lo que actualmente los trámites se continúan resolviendo en la versión anterior (sin TAD y con firma electrónica).

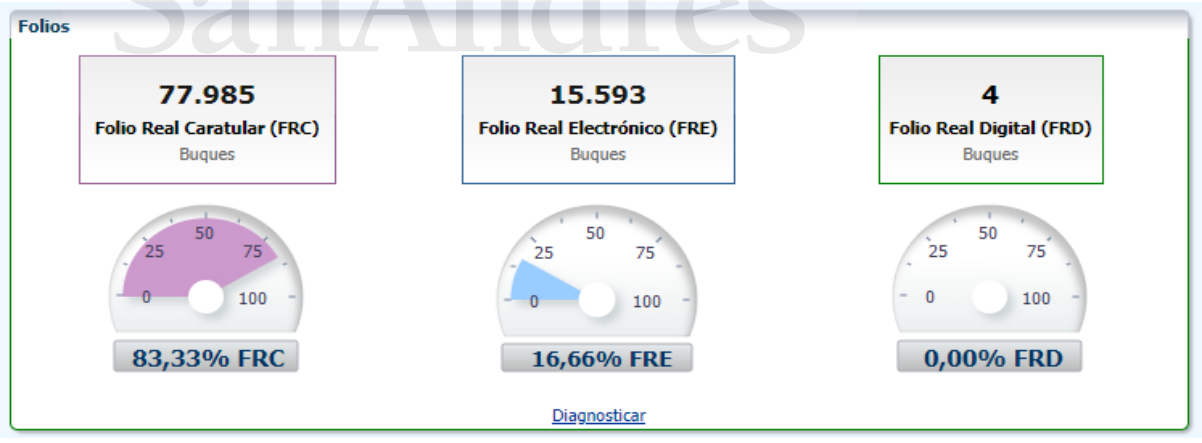


Ilustración 29 - Situación por tipo de folio (8/4/2020)

Capítulo 5 - Solución propuesta

Oportunidades de las mejoras en los procesos

Como hemos visto en el capítulo anterior, se han logrado grandes avances en la gestión de los trámites del registro de buques; sin embargo se considera que existen condiciones que generan oportunidades de mejora:

- La cantidad de expedientes originados en TAD es escasa y en consecuencia la cantidad de folios reales digitales casi nula, ya que su generación se encuentra ligada a la versión del gestor de modelado de proceso (BPM) asociado a la iniciación del expediente desde TAD. Esta proceso se implementó formalmente a fines de 2019, pero en la práctica evidentemente no está siendo plenamente utilizado. La causa de esta infrautilización es consecuencia de los problemas que persisten desde la implementación de los trámites en la plataforma de TAD; ya que los procesos no han sido profusamente testeados y se aprecian fallas que generan dificultades al usuario. Debido a este inconveniente (y también por costumbre), es normal que el usuario ocurra directamente al punto de atención al público en la agencia jurisdiccional o en el registro central para resolver el trámite documental y realizar en el mismo acto la verificación técnica si así correspondiere.

- Otro inconveniente asociado a TAD, es que una vez iniciado el trámite, se debe esperar la conciliación contable del pago efectuado a través de eRecauda, antes que se pueda generar el expediente electrónico en GDE, para que así pueda avanzar la agencia/registro en su tramitación. La conciliación contable es un proceso que lleva varios días, ya que demanda 72 hs de clearing bancario y los tiempos que insumen los procesos de los sistemas administrativos internos.

- El proceso en uso (sin TAD) comprende la emisión del folio real con la firma electrónica del oficial del registro que estableció la sesión. Señalamos anteriormente, que se considera firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por un signatario como su medio de identificación, que carece de alguno de los requisitos legales para ser considerada firma digital; y si ésta es desconocida por su autor, corresponderá a quien la invoca acreditar su validez. De este modo, corresponderá al administrador del sistema, proveer oportunamente los elementos técnicos de juicio que permitan acreditar la validez. La custodia de la base de datos, logs y repositorio de documentos (pdf), está bajo su dominio y exclusiva responsabilidad.

- El proceso de migración y normalización de la base de datos (de SIB a PROGEBU), se va produciendo en la medida que se tramitan los expedientes; por lo que la actualización de la base de datos podría tardar años. Hasta entonces carecerá de la necesaria consistencia y confiabilidad.

Planteo de las mejoras a introducir en los procesos.

Para la eficiente gestión del Registro de Buques, y en base a las oportunidades de mejora detectadas, se debería adoptar el siguiente esquema de mejoras:

- Tomar contacto con los responsables de TAD a fin de perfeccionar los trámites oportunamente implementados. En principio se debe asegurar que los trámites fluyan de manera apropiada y se corrijan todos los inconvenientes que está presentando la plataforma. Si bien no vamos a detallar todas las correcciones que se deben practicar en TAD; a modo de ejemplo, se sugiere que solo los trámites que requieren de alguna verificación técnica debieran ser derivados por el sistema a la agencia más próxima al "puerto de asiento", que consigna el usuario al solicitar el trámite. Aquellos en que no es necesaria ninguna verificación técnica, deberían ser derivados directamente al Registro, ya que la agencia no agrega valor y solo ocasiona pérdida de tiempo.

- Los trámites deberán poder continuar sin tener que esperar la conciliación bancaria. Es suficiente con que el usuario adjunte el comprobante de pago antes de la resolución del trámite; dejando el asunto de la conciliación bancaria de los pagos para su control en otro subsistema o parte del proceso (ejemplo antes de permitir archivar el expediente).

- Firmar digitalmente en GEDO el folio real: una vez preparado el pliego del folio en el sistema PROGEBU, se envía al ecosistema de GDE para que el oficial de registro actuante firme digitalmente el documento. Este documento se almacena en el Repositorio Único (REPU) de GDE. Se genera así el Folio Real Digital (FRD).

- Efectuar un sellado de tiempo de un hash o digesto criptográfico (DC) del Folio Real Digital (FRD) en la Blockchain Federal Argentina (BFA) para garantizar, tanto al Registro como al Administrador del sistema (GDE), que el folio real digital firmado y almacenado en el entorno GDE-RUDO, no ha sido alterado y que dicho documento se incorporó en la cadena en un determinado momento dando pruebas de su existencia e integridad.

- Se debe completar el proceso de migración y normalización de la base de datos (de SIB a PROGEBU) en forma independiente de los trámites, para que la base de datos PROGEBU en el menor tiempo posible sea totalmente consistente y confiabilidad, Se propone un procedimiento abreviado a tal fin.

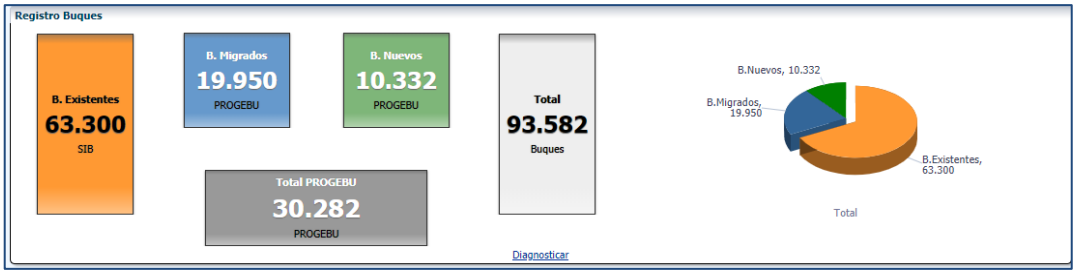


Ilustración 30 - Estado de la migración (8/4/2020)

En base a estas consignas, se adjuntan los correspondientes cursogramas que señalan el flujo de los procesos indicados.

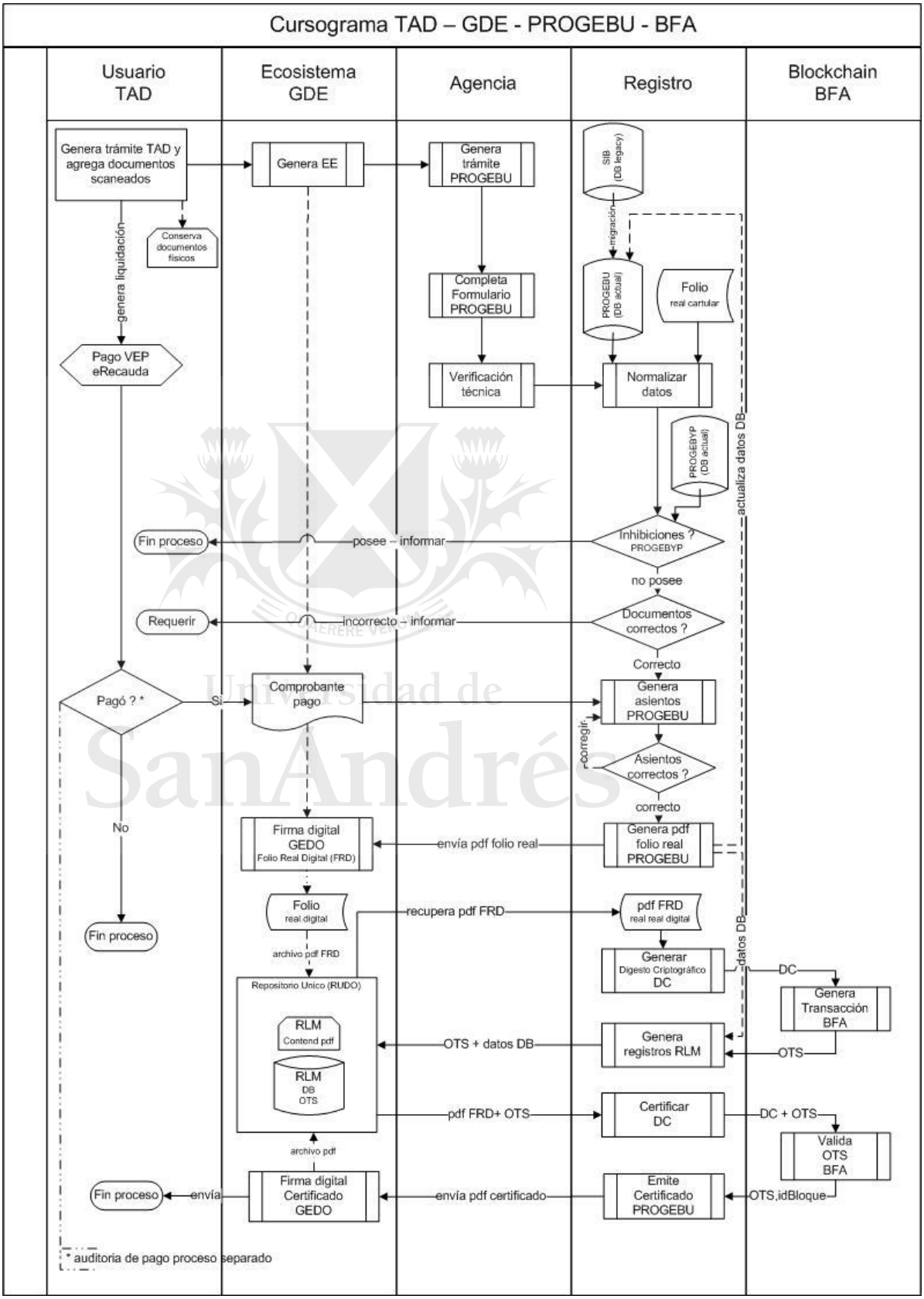


Ilustración 31 - Cursograma de trámite modelo propuesto con blockchain (Elaboración propia)

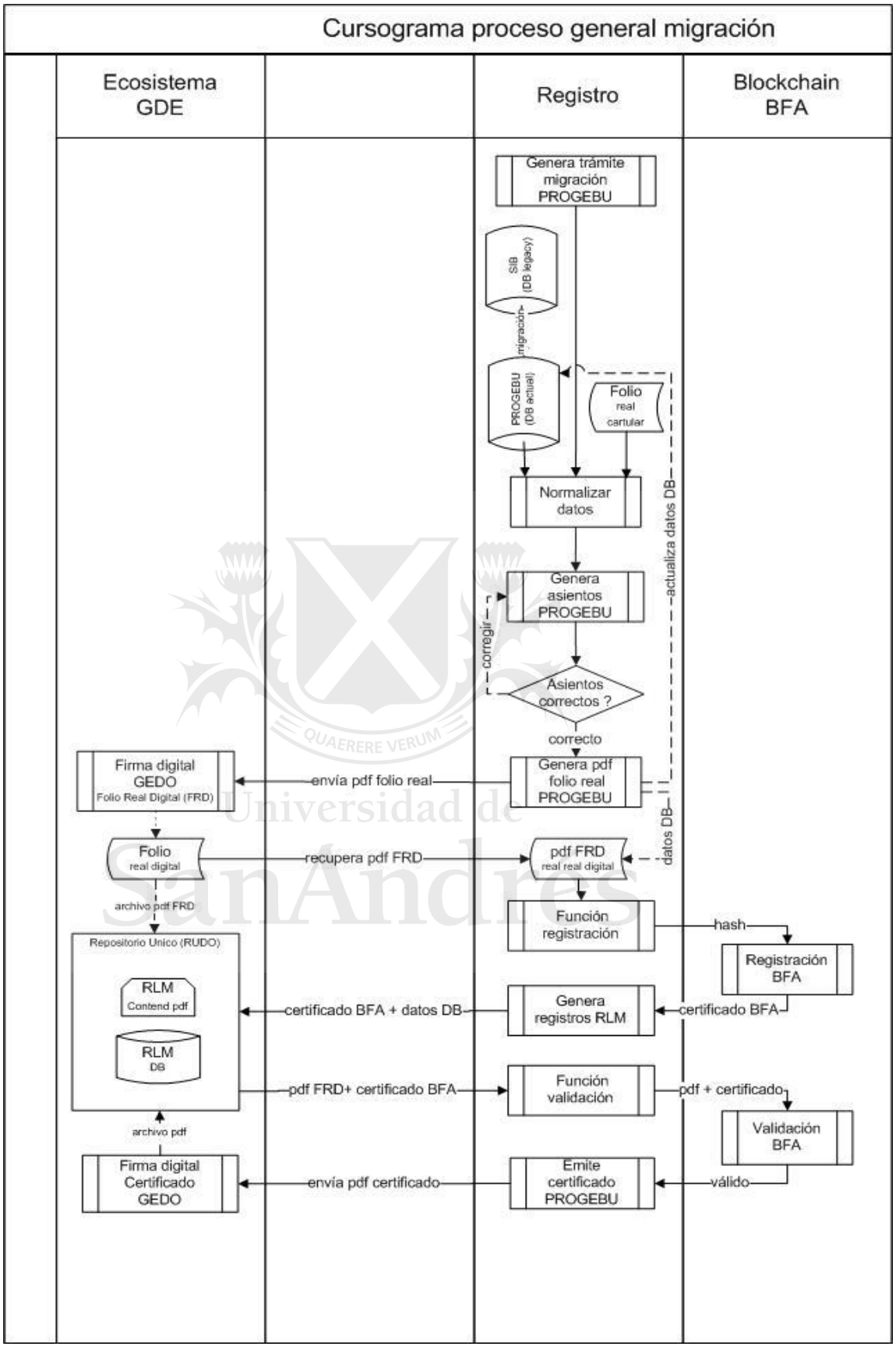


Ilustración 32 - Cursograma del proceso de migración general (Elaboración propia)

Justificación de las mejoras aportadas

Las propuestas de las mejoras expuestas, se justifican en las siguientes premisas:

- La utilización de la plataforma TAD, no sólo resulta mandatorio en función de la resolución que impuso su implementación; sino que su efectiva adopción mejorará la experiencia del usuario a la hora de realizar trámites ante la administración pública nacional y más específicamente ante el Registro. Los inconvenientes que dificultan su utilización deben ser rápidamente planteados ante los responsables de la plataforma TAD, aportando los pedidos de mejora en base a profundo trabajo de testeo y brindar el acompañamiento de un equipo de trabajo comprometido con los objetivos que asegure su pronta y efectiva resolución.

- Tal como está implementado actualmente el proceso en TAD, que impide la prosecución del trámite hasta tanto no esté conciliado el pago ya que no se genera el expediente electrónico (EE) en el ecosistema GDE, imposibilita que el Registro avance en la resolución del trámite con tiempos improductivos que no agregan valor al proceso. Al no existir un EE, tampoco se podría eventualmente asociar en forma electrónica el pago realizado en eRecauda. Se considera que es suficiente, con que el usuario adjunte el comprobante del pago, antes de que el Registro se disponga a concluir el expediente para dar curso al trámite. Cualquier cuestión referida a la conciliación contable, debería ser tratada por fuera del trámite principal.

- Teniendo la disponibilidad para usar firma digital, el empleo de firma electrónica para rubricar documentos que son actos administrativos, deja de ser una opción; ya que los documentos firmados digitalmente en GEDO tienen la misma validez jurídica y probatoria que aquellos documentos firmados en forma ológrafa, y se evita, como ocurre con la firma electrónica, cualquier proceso posterior de acreditación de validez.

  Sumamos a esto la ventaja que representa firmar digitalmente en el entorno GDE, que le agrega su esquema de protocolización, almacenamiento y conservación de documentos.

- La posibilidad de efectuar el “sellado de tiempo” en la cadena de bloques de Blockchain Federal Argentina (BFA) de un digesto criptográfico del FRD creado por personal del Registro de Buques y almacenado en el ecosistema GDE, resuelve cualquier desafío de confianza que pudiera existir entre la partes (la registral y la de sistemas). La blockchain brinda la posibilidad que cualquiera de ellas pueda, en cualquier momento, comprobar con el hash del documento, la fecha y hora en que fue registrado en la cadena y certificar de manera fehaciente la integridad y autenticidad del mismo; lo que le da total transparencia y trazabilidad al proceso.

  La firma digital del folio da certeza sobre la autoría y el contenido, lo que complementado con el sellado de tiempo del digesto criptográfico de ese folio real en la cadena de bloques, brinda certeza de su existencia a partir de un determinado momento. Hay un elemento de control ajeno a cualquiera de las partes – el registro que firma y el área de sistemas que almacena -, que actúa como un tercero de confianza y garantiza la transparencia de la operación para ambas partes. El profesional del registro con la firma digital asume la autoría y el contenido del folio; en tanto que los responsables del sistema deben velar por su integridad y conservación en al dispositivo de almacenamiento. La inclusión del hash del folio en la cadena de bloques,

permite demostrar la integridad y existencia del documento a partir de determinado momento, lo cual puede ser auditado en forma pública y abierta.

Dado que es prácticamente imposible borra datos incluidos en la cadena de bloques, el hecho solo se incluya un digesto criptográfico del documento y no el documento propiamente dicho, asegura que no se viole cualquier norma regulatoria de protección de datos. El almacenamiento de la información sensible es fuera de la cadena de bloques (off-chain). La blockchain no es una nube de almacenamiento de archivos; sólo se almacenan los hash de los documentos que se quieren garantizar.

En el caso de necesitarse clonarse o duplicarse un documento, la certificación del mismo puede hacerse en la cadena de bloques sin necesidad de intermediación de terceros de confianza. Esto será de gran utilidad en la medida que se extienda su uso y haya mayor cantidad de aplicaciones que interoperen electrónicamente.

- Hasta tanto no se complete el proceso de migración y normalización de la base de datos (de SIB a PROGEBU), el Registro y la Prefectura no contarán con un registro electrónico consistente y confiable, necesario para todos sus procesos y de terceras organizaciones (tributarias, judiciales, administrativas, etc), por lo que se debe priorizar e independizar de la gestión documental del Registro.

Recurso técnico utilizado en la propuesta

El recurso técnico que aún no se encuentra implementado en el proceso es el sellado de tiempo, por eso se procederá a explicar el procedimiento que ampara esta solución.

El sellado de tiempo es un servicio de propósito general que permite demostrar la existencia de alguna información (en este caso el hash del documento) antes de determinada fecha, sin la posibilidad de que el dueño pueda modificar ese sellado de tiempo. La cadena actúa como una autoridad de sellado de tiempo independiente y confiable.

En este caso, la implementación del estampado del “sello de tiempo” en el hash del folio real digital para brindar total transparencia y trazabiliadad al proceso, y se hace basándose en una API REST que se encuentra disponible en la cadena y facilita el desarrollo de aplicaciones que quieran conectarse a la blockchain BFA. Esta API REST posee dos EndPoint: ‘Stamp’ para registrar el hash en la blockchain y ‘Verify’ para verificar la misma.

En la aplicación PROGEBU se programa el código que recupera del GDE el folio real digital allí firmado y almacenado, y se genera el digesto criptográfico mediante una función hash (en este caso HASH256); el cual se envía a la interfaz web para end-users que enmascara la API disponible en BFA y que brinda la funcionalidad que permite insertar el hash o verificar si el comprobante digital previamente emitido por BFA es válido.

El EndPoint ‘Stamp’ de la API-REST tiene la capacidad de recibir el digesto criptográfico (DC), generar un OpenTimeStamp (OTS) temporal que funciona como un comprobante digital temporal que devuelve a la aplicación. La API invocar en forma asincrónica al nodo transaccional y ejecuta el Smart Contract ‘Stamp´ que genera una transacción que termina impactando el DC en un bloque de la blockchain.

El End-Point ‘Verify’ de la API-REST, funciona en forma sincrónica y recibe desde la aplicación el DC y el OTS (temporal o definitivo).

Si el OTS es temporal, se invoca el Smart Contract 'Verify' que verifica si la transacción ya se ha ejecutado. Si no lo ha hecho devuelve estado: 'Failure'; caso contrario verifica si el DC impactó en el bloque, y si aún no lo ha hecho devuelve estado: 'Pending'. Si ya lo ha hecho, con el valor del OTS recupera el idBloque y el DC almacenado en la blockchain. Después compara el DC que recibió de la API y el almacenado; si son iguales devuelve Estado 'Success' y el idBloque, caso contrario Estado: 'Failure'.

Si el OTS es definitivo (DC ya impactó en la blockchain), se invoca el Smart Contract 'Certify' se recupera el idBloque y el DC almacenado en la blockchain y se comparan los DC (recibido y almacenado). Nuevamente, si son iguales devuelve Estado 'Success' , el idBloque y el OTS (OpenTimeStamp) o Estado: 'Failure'.

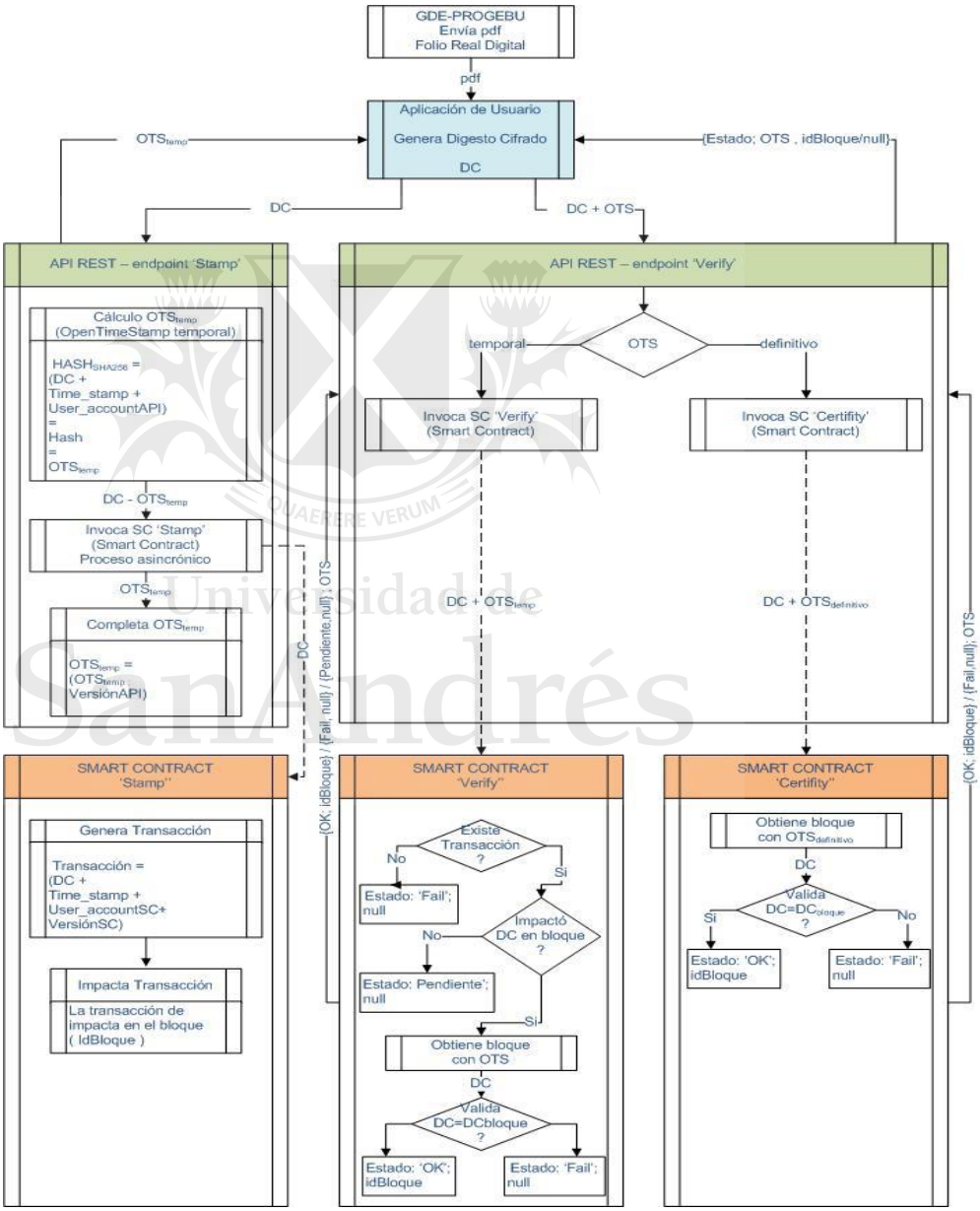


Ilustración 33 - Diagrama Open Time Stamp BFA (Elaboración propia en base a (BFA, 2020))

API Rest

Endpoint Stamp

- Método: POST
- Content-Type: application/json
- Endpoint: /api/tsa/stamp/
- Parámetros:
  - file_hash: hash del archivo en formato sha256
- Respuesta:
  - success: Devuelve el ots temporal
  - failure: Devuele el mensaje de error
- Ejemplo:
  - { "file_hash": "1957db7fe23e4be1740ddeb941ddda7ae0a6b782e536a9e00b5aa82db1e84547" }

Endpoint Verify

- Método: POST
- Content-Type: application/json
- Endpoint: /api/tsa/verify/
- Parámetros:
  - file_hash: hash del archivo en formato sha256
  - ots: ots temporal o definitivo devuelto por el stamp o el verify
- Respuesta:
  - success: Devuelve el ots definitivo y un mensaje indicando el archivo, el número de bloque donde fue ingresado y fecha y hora
  - pending: Devuelve un mensaje indicando que la transacción está pendiente de subida a la blockchain
  - failure: Devuelve el mensaje de error
- Ejemplo:
  - { "file_hash": "1957db7fe23e4be1740ddeb941ddda7ae0a6b782e536a9e00b5aa82db1e84547", "ots": "NzNkYzA5OGJkODlmZjdlMjc4OGFjMzJlNmU2ODdiOTdmODdiMTBjMWIyNzg5OTFlMDNkN2E2YWVkMDk3ODJkZTAxLTB4NGM2ZmNiNDBhMmUyZGVjYzc2YWQzMjM3MDU2NzZjMjljYWE1MmIyYjZkMDdiMDIzYjBhY2EzOWYzZGIxYmRlZg==" }

Ilustración 34 - Ejemplo API REST - (BFA, 2020)

Funcionamiento de la API en GUI pública

Si bien, no se encuentra aún implementada en la aplicación PROGEBU las llamadas a la API de referencia; se puede a efectos de la demostración, utilizar las llamadas a dichas API que se hacen desde la GUI de la web de Blockchain Federal Argentina:

Ilustración 35 – GUI Sellar BFA

1. Sellar: Se arrastra el documento (FDR) que se quiere sellar y se observa el hash creado del mismo. Como resultado de la operación se obtiene el recibo temporal correspondiente al archivo.

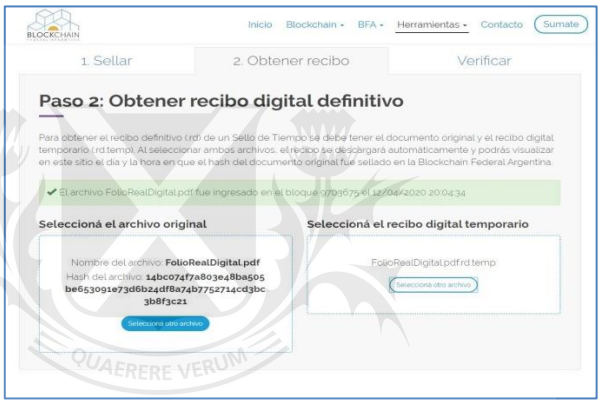


Ilustración 36 – GUI Obtener recibo BFA

2. Obtener recibo: Se selecciona el archivo original y el recibo temporal. La aplicación devuelve la indicación que el hash del archivo fue ingresado en el bloque y la fecha-hora. Si aún no fue ingresado, indicará que el mismo está pendiente.

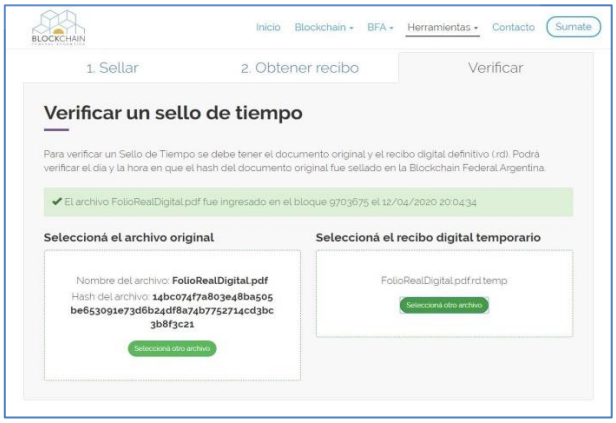


Ilustración 37 - GUI Verificar BFA

3. Verificar: Se selecciona el archivo original y el recibo definitivo. La aplicación devuelve el número de bloque en que el hash del archivo ha sido ingresado y la fecha-hora.

Capítulo 6 - Resultados y conclusiones

Resumen de la investigación

El presente trabajo de investigación se basó en la necesidad de mejorar y optimizar las características de seguridad e inmutabilidad del Folio Real, producto del proceso de modernización y sistematización adoptado por el Registro Nacional de Buques, y verificar si la tecnología blockchain puede contribuir en ese objetivo.

En este contexto, se ha repasado la situación imperante en los registros correspondientes a las mayores flotas mundiales para comprender el estado del arte en dichas instituciones. Para ello, en base al informe estadístico anual 2019 de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), organismo de la Asamblea General de la ONU, se determinaron las mayores flotas y se realizó un estudio de los sistemas utilizados.

De este estudio se puede corroborar que los países que embanderan las mayores flotas, no son necesariamente las economías propietarias de los buques; e inscriben sus buques en registros altamente dinámicos, generalmente asociados con la registración de empresas off-shore, haciendo una combinación que resulta sumamente apropiada para el eficiente desarrollo del transporte mundial por buques que comprende más del noventa por ciento de todo el comercio mundial.

Entre estos Registros encontramos los de Panamá, Liberia, Islas Marshall, Hong Kong y Singapur; todos ellos con gran desarrollo normativo y tecnológico, lo que resulta imprescindible para que mantengan su nivel de eficiencia y sigan siendo preferidos por los Armadores[44] . Poseen sistemas informáticos bien implementados, sin embargo, sólo en el caso de Singapur hemos encontrado que se desarrollan iniciativas para el uso de la tecnología blockchain, la cual estaría disponible en el presente año. Esta iniciativa está siendo desarrollada con el auspicio de la Cámara de Comercio Internacional (ICC) y pretende ser un modelo de escala internacional.

También es destacable mencionar el caso de Dinamarca, sede del mayor operador de buques del mundo y con un registro nacional de respetables dimensiones, y que también está desarrollando un proyecto para digitalizar el comercio y los procesos de registro de buques utilizando tecnología blockchain, como parte de una estrategia gubernamental para impulsar el crecimiento digital en Dinamarca y que también estará disponible para mediados de 2020.

En el proceso de investigación hemos abordado también la situación de los Registros de Propiedad de Tierras o Bienes Inmuebles; ya que por sus características se asemejan mucho en complejidad a los registros de buques. En este caso, con mayor fortuna, advertimos que son diversos los países que han avanzado con el uso de la tecnología blockchain para encarar la modernización y sistematización de sus registros.

En esta situación encontramos a Estonia, el primer país que implementó su propia tecnología blockchain para mejorar la administración pública y con ello la gestión de oficinas gubernamentales y diversos registros, que ya ha alcanzado un nivel de madurez realmente importante con su infraestructura de firmas sin claves (KSI blockchain) y su plataforma de inter-operatividad (X-tree). Este

[44] Armador: es la persona o empresa naviera que se encarga de equipar, aprovisionar, dotar de tripulación y mantener en estado de navegabilidad un buque de su propiedad o bajo su posesión, con objeto de asumir su gestión náutica y operación comercial.

caso es interesante, ya que Estonia adoptó una solución ajustada a sus necesidades dado que no necesitan construir un sistema de confianza cero, porque depende de autoridades confiables.

El Reino Unido es otro ejemplo de similares características; y así encontramos otros ejemplos destacables como las implementaciones en Japón, Suecia y la República de Georgia, que están avanzando en programas de modernización y mejoras en la gestión de sus registros de tierras usando tecnología blockchain.

En cuanto a los aspectos tecnológicos, si bien este trabajo pretende abordar la temática desde un punto eminentemente funcional; se exploran los argumentos técnicos en los que se basa esta tecnología, para que el lector tenga una acabada idea de los elementos y complejidad que intervienen que cada una de las versiones de esta tecnología.

Se destacan los principales conceptos y definiciones que involucran blockchain/DLT, métodos de consenso y principales aplicaciones, y se procura abarcar la mayoría de las implementaciones. Así encontramos la génesis en Bitcoin, para pasar luego a Ethereum, Quorum, Hyperledger, redes POA y terminamos en la Blockchain Federal Argentina, reflejando en cada uno de ellas sus fortalezas y debilidades.

Seguidamente, se repasaron los aspectos legales relativos a la organización del Registro de Buques, y luego a las normas generales del Estado, que atañen a la problemática planteada. Así partimos de la ley de firma digital, y las sucesivas normas que plantean fundamentalmente la reforma administrativa del Estado; muchas de ellas de reciente implementación y que han facilitado en mucho la modernización de muchas estructuras de gestión del Estado y fueron un factor decisivo en muchas de las mejoras implementadas en el Registro.

En el siguiente capítulo, se desarrolla la situación imperante en relación al sistema del Registro de Buques; partiendo de su situación inicial y las mejoras introducidas durante su transición al sistema actualmente en uso, y que conduce al estado en que se requiere la necesidad de mejorar y optimizar las características de seguridad e inmutabilidad del Folio Real allí generado.

En función del análisis de estos procesos, se detectan oportunidades de mejora, se plantean las mejoras en los procesos y se justifican estos aportes. También se explicitó técnicamente la funcionalidad del sellado y a grandes rasgos como se implementa.

Universidad de San Andrés

Conclusiones

A. Objeto de la presente investigación

Conforme el desarrollo del presente trabajo, se puede garantizar que la tecnología blockchain resulta apropiada para garantizar la prueba de existencia de un folio real digital en el registro nacional de buques, mediante el "sellado de tiempo" del hash del documento.

La tecnología blockchain, usada como complemento de la firma digital, resuelve cualquier desafío de confianza y certifica de manera fehaciente la integridad y autenticidad del documento, brindando transparencia y trazabilidad al proceso.

Ofrece certeza de la existencia del folio real a partir de un determinado momento; permitiendo que esto sea auditado en forma fácil, pública y abierta.

Asegura que no se viola ninguna norma regulatoria de protección de datos, ya que el almacenamiento de la información sensible se efectúa fuera de la cadena de bloques (off-chain) y solo se agrega a la cadena pública un hash del documento.

La tecnología blockchain que se considera más adecuada en estas circunstancias, es el uso de la Blockchain Federal Argentina, que es una blockchain implementada sobre Ethereum, permisionada con consenso de Prueba de Autoridad, sin cripto-monedas asociadas, abierta y sin cargos de operación, que es mantenida y operada por un consorcio de instituciones, organizaciones, empresas y organismos argentinos interesados en su desarrollo. La red se encuentra desplegada, en plena operación y la Prefectura integra dicho consorcio.

Universidad de SanAndrés

B. El desarrollo de blockchain en la industria marítima a nivel global.

Como vimos, el informe de Gartner (Gartner, 2019) predice que el impacto comercial de blockchain será transformador en la mayoría de las industrias en un lapso de cinco a diez años y, específicamente en el campo del comercio mundial, donde podemos posicionar a los registros de buques mercantes, observamos que es incipiente la adopción de esta tecnología por parte de los actores más pujantes y desarrollados del sector.

Esta incipiente adopción que se menciona, la podemos apreciar en iniciativas como la propuesta por la Cámara Internacional de Comercio y la Asociación de Navegación de Singapur, que están trabajando activamente para desarrollar el Registro Internacional Electrónico de Buques (IERS) de Singapur basado en blockchain y que pretende ser un modelo para los demás registros del mundo; o en la decisión de Maersk, el mayor operador marítimo mundial, que se asoció con IBM para desarrollar una plataforma para ser utilizada por todo el ecosistema global de envíos con la intención de proporcionar una mayor eficiencia y seguridad en el comercio mundial utilizando la tecnología blockchain. También se puede destacar el proyecto en el que Ernest&Young, Guardtime y Microsoft, que participan en la implementación de la plataforma basada en blockchain llamada "Insurwave" y que está dirigida a transformar el proceso de gestión de riesgos del mercado de seguros para más de 1000 embarcaciones comerciales. En este proyecto Maersk colaboró no sólo en su desarrollo, sino que actualmente actúa como el cliente piloto con su cartera de cascos marinos.

Otra manera efectiva de utilización de las cadenas de bloque en la industria naviera, la podemos encontrar en los Libros de Registros Electrónicos de Hidrocarburos, donde se pretende establecer un estándar en materia de transparencia, credibilidad y trazabilidad de las operaciones de todos los productos oleosos que se manipulan en los buques, y que ha tenido el reconocimiento de la Organización Marítima Internacional, de las principales sociedades de clasificación y registros de buques más importantes del mundo.

Como se advierte, estas soluciones basadas en blockchain en el campo del transporte marítimo, está siendo fuertemente apoyada por los más importantes actores del mercado, y conforme se vayan constatando los éxitos de estas implementaciones, podremos esperar su evolución y una adopción más vigorosa en otros segmentos de la industria.

Pero para que todo ello suceda, se requiere de mayor protagonismo e implicancia de distintos actores que influyen en la gobernanza del despliegue tecnológico, pero también comprometidos con los intereses de los negocios y las acciones relativas a la toma de decisiones.

Si bien blockchain se ofrece como una solución tecnológica descentralizada e inmutable de base de datos, lo cierto es que la realidad dicta que - tanto en BitCoin como en Ethereum -, se produjeron vulnerabilidades o faltas de acuerdos, que han provocado escisiones o rupturas, en las que han intervenido decididamente los curadores de la red. Son estos actores que cuentan con una relativa especialización, discuten las mejoras en el código, previenen ataques y proponen las nuevas implementaciones, los que tienen una fuerte influencia en el destino de la red y manejan cierto grado de centralización.

También, existen quienes intervienen en la programación de los tokens, contratos inteligentes, oráculos y aplicaciones. Todas estas piezas de software, en cuánto creaciones humanas, no están exentas de contener errores de programación; fallos que pueden afectar derechos de los particulares que operan en la red.

No vamos abordar la discusión jurídica que deriva de la afectación de derechos en base a las aplicaciones que se auto-ejecutan en la cadena de bloques sin intermediarios; solo indicar que existe una diversidad de posibilidades basadas en los diferentes casos de uso y las normas del derecho y jurisdicción que son aplicables en cada uno de estos casos. En este sentido, cabe también señalar que los cambios tecnológicos imponen un desafío para los legisladores y juristas, que deben asumir el reto de regular y adaptar las normas del derecho a las realidades y posibilidades de progreso que suponen estos cambios tecnológicos. En definitiva, es necesario adaptar el marco jurídico para brindar certeza y evitar futuros conflictos que deriven del uso de la red.

El involucramiento de organizaciones normalizadoras, organismos multilaterales y la propia participación de cada Estado, resultarán necesarios para dirimir y resolver fricciones derivadas de los intereses y expectativas de las partes. La participación de las administraciones públicas en la adopción de esta tecnología, ayudará a extender su utilización en sus circuitos de gestión interna de los gobiernos, facilitando también que los procesos fluyan apropiadamente entre los sistemas estatales y empresariales. Las tecnologías de información y comunicaciones (TIC) hoy ofrecen a las administraciones públicas la posibilidad de poner en prácticas programas de modernización y simplificación administrativa que permiten agilizar los procesos y consolidar gestiones más abiertas, confiables y transparentes, y blockchain promete ser un elemento esencial en este proceso.

La República de Estonia, es un claro modelo de país digital, donde los sistemas de información estatales se encuentran estructurados sobre la plataforma de intercambio de datos X-tree (antes X-Road) basada en la infraestructura de blockchain (KSI infraestructura). Esta verdadera autopista digital, proporciona en forma estandarizada y segura la posibilidad de implementar y consumir servicios electrónicos, garantizando confidencialidad, integridad e seguridad para el necesario intercambio de información con las empresas y ciudadanos en general y entre organismos del Estado entre sí. Este fue el primer país en implementar tecnología DLT/blockchain y se ha transformado después de unos años, en la más avanzada sociedad digital del mundo.

Más allá del incuestionable suceso que han tenido las criptomonedas basadas en blockchain; lo cierto es que en otro tipo de aplicaciones todavía se transita por la implementación de modelos experimentales y aún no se ha alcanzado toda su potencialidad. Hay un fuerte compromiso con la investigación y el desarrollo de nuevas redes y aplicaciones tratando de resolver de mejor manera los desafíos que representan nuevos casos de uso; es un mundo en ebullición todavía, que recién despega y que está en un estado de cambio permanente. Esta actividad está dejando las necesarias enseñanzas y lecciones que llevaran a la depuración del sistema y prevalecerán las mejores soluciones; condición necesaria para ir alcanzando ciertos consensos y grado de normalización, para que las aplicaciones y sus derivados sean portables e interoperables y así poder escalar.

QUAERERE VERUM
Universidad de
SanAndrés

Capítulo 7 – Reflexión final y futuras líneas de investigación.

Reflexión final

Cuando imaginamos los elementos que debería contener un sistema de gestión del Estado moderno y eficiente, pensamos en una estructura similar a la siguiente:

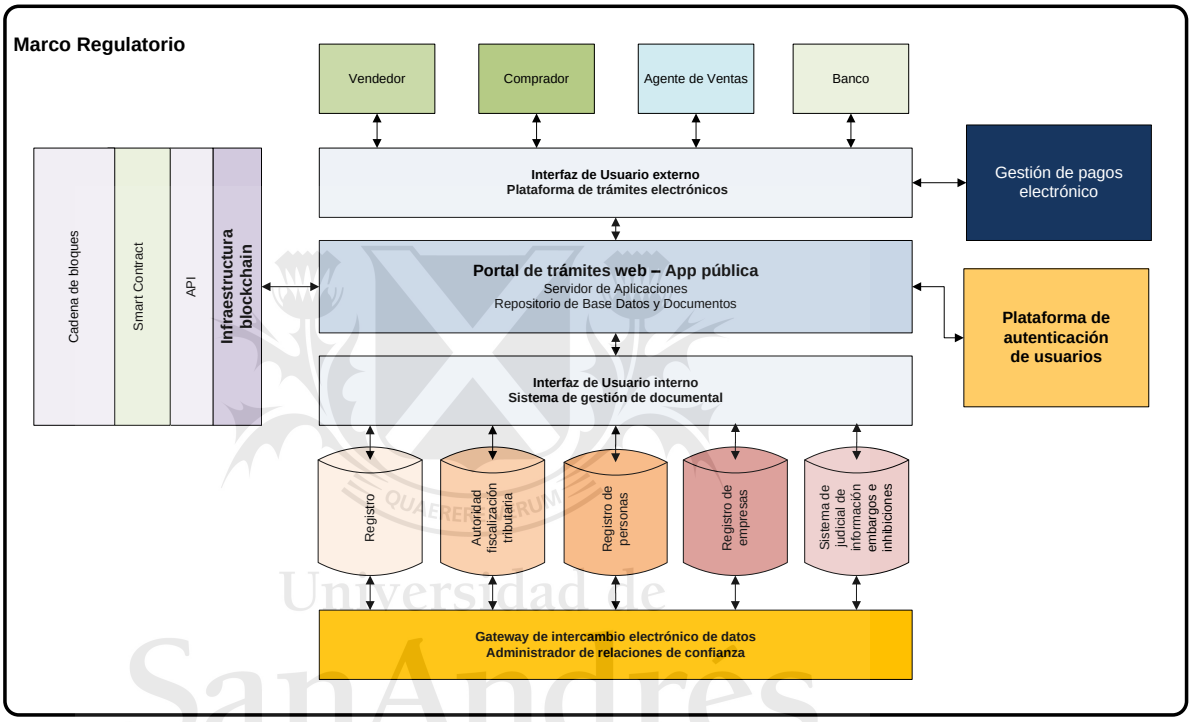


Ilustración 38 -Ecosistema ideal

Desagregando esta imagen, destacamos que en principio que resulta necesario contar con un marco regulatorio actualizado y que adopte las nuevas tecnologías disponibles; permitiendo así la elaboración de nuevos procesos que comprenden firmas digitales, pagos electrónicos y gestión de trámites a distancia.

También es necesario que el Estado disponga de una plataforma centralizada de trámites, accesible a todos los ciudadanos por web o una App en el celular. Esa plataforma debe disponer los recursos de infraestructura informática y de telecomunicaciones, que soporten sistemas y aplicaciones donde se desarrollen los trámites de los diferentes organismos.

Esa infraestructura de hardware y software, debe exponer una interfaz externa para que los ciudadanos accedan a los trámites disponibles, y otra interna, para que los funcionarios gestionen los expedientes relacionados con esos trámites. Para ambos tipos de usuarios, se debe contar con una plataforma de autenticación de usuarios, en la que se puedan enrolar directamente y permita federar los proveedores de identidad disponibles.

Asimismo se debe contar con una plataforma de pagos electrónicos, que permita acceder a los canales habituales o de forma presencial ante la ventanilla de los bancos.

Los organismos del Estado deberán poder intercambiar datos electrónicamente en forma automática, y para ello es preciso establecer las relaciones de confianza entre los organismos, que permitan brindan el acceso a los datos necesarios para sus operaciones.

Finalmente, se debe contar con una infraestructura que administre y resuelva cualquier cuestión de confianza que pueda existir entre las partes.

Si observamos todo los sistemas que interactúan en los procesos descriptos en el presente trabajo, vemos que el Estado mucho ha avanzado en la instrumentación de los componentes mencionados en el esquema anterior. Para ser más claros, ponemos nombres propios a los módulos disponibles en nuestro país para tener una real dimensión de la situación actual:

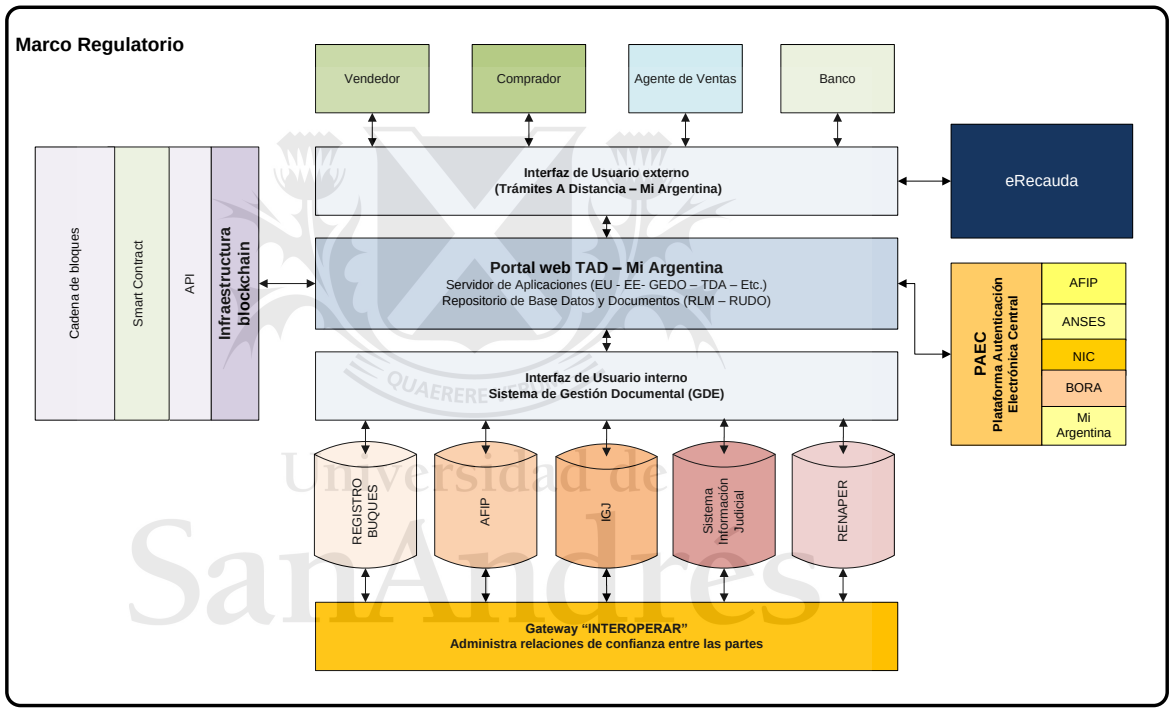


Ilustración 39 -Ecosistema real

Como podemos advertir, la mayoría de los componentes que ya están disponibles fueron implementados a nivel de administración central (GDE, TAD; PAEC, eRecauda, RLM/RUDO, etc) y en los sistemas de los organismos más desarrollados informáticamente (AFIP, ANSES, RENAPER). Es preciso continuar con el esfuerzo en el resto de los organismos del Estado, motivándolos y asistiéndolos para que definitivamente entre todos se puedan alcanzar los objetivos deseados.

Cuando analizamos el proceso del registro de buques, vimos que se hace uso de casi todos estos módulos y que aún hay que continuar trabajando en resolver las relaciones de confianza que imposibilitan un fluido intercambio electrónico de datos entre organismos, para así poder implementar contratos inteligentes en la infraestructura blockchain que permitan avanzar en un gobierno electrónico más transparente, dinámico y eficiente.

Futuras líneas de investigación

En el desarrollo de este trabajo, hemos comentado brevemente respecto la tokenización de los activos digitales. La tokenización consiste en la creación en blockchain de un “token digital” que representa un activo real, sean estos financieros, inmuebles, obras de arte, archivos de multimedia, etc., en fin, casi cualquier elemento existente en el mundo real puede ser representado como un token digital.

Estos token no solo sirven para almacenar en una blockchain datos asociados a su ciclo de vida, sino que son especialmente útiles para realizar operaciones sobre las cadenas. Los token son de gran relevancia ya que pueden ser utilizados para aumentar la velocidad de las transacciones, incrementar la transparencia y producir una reducción de costos de las transacciones.

Analizar sus beneficios y las dificultades en su implementación, como se aborda esta entidad desde lo legal y regulatorio, cuáles son sus casos de uso y en qué contexto; y todo lo que rodea a esta temática merece del desarrollo de futuras líneas de investigación, ya que están íntimamente ligados e influyen profundamente

QUAERERE VERUM
Universidad de
SanAndrés

Capítulo 8 – Tablas y referencias

Tabla de Ilustraciones

QUAERERE VERUM
Universidad de
SanAndrés

Referencias

Guba, E., & Lincoln, Y. (2002). Paradigmas en competencia en la investigación cualitaiva. *Por Los Rincones. Antología de Métodos Cualitativos En La Investigación Social.*

Acha, H. R. (Núm. 19 de Vol. 7 de 2013). *AEQUITAS Virtual -- USAL.* Obtenido de Publicación del la Facultad de Ciencias Jurídicas : https://p3.usal.edu.ar/index.php/aequitasvirtual/article/view/1360/1720

AMP. (16 de 09 de 2019). *El Registro de Naves de Panamá moderniza el registro de naves.* Obtenido de https://panamashipregistry.com/registry-news/panama-ship-registry-modernizes-ship-registration/

Asian Legal Information Institute. (06 de 03 de 2020). *Laws of the People's Republic of China*. Obtenido de http://www.asianlii.org/cn/legis/cen/laws/rgtros490/

Bakhoff, M. (2014). *Consensus algorithms for distributed systems.* Obtenido de http://ds.cs.ut.ee/courses/course-files/MartBakhoff-consensus.pdf

Baran, P. (1964). *On Distributed Communications.* Rand Corporation.

BFA. (18 de 03 de 2020). *Blockchain Federal Argentina.* Obtenido de Tecnología: https://bfa.ar/bfa/tecnologia

BFA. (06 de 04 de 2020). *GitLab BFA.* Obtenido de https://gitlab.bfa.ar/public: https://docs.google.com/document/d/19PYSiAkInGXLEbSDqWQh-1zSrY4rr20Palr1H8MjaEQ/edit

Bielli, G. E. (03 de 06 de 2019). *Terceros de confianza y certificación de prueba electrónica.* Obtenido de https://iadpi.com.ar/index.php/2019/06/03/terceros-de-confianza-y-certificacion-de-prueba-electronica/

Bielli, G. E., & Ordoñez, C. (2019). *La Prueba Electrónica; Teoria y Práctica.* La Ley.

Bit2me. (s.f.). *Academy .* Obtenido de https://academy.bit2me.com/que-es-hash/

Bit2me Academy. (21 de 03 de 2020). *Qué es una clave privada.* Obtenido de https://academy.bit2me.com/que-es-clave-privada/

Bitcoinist. (10 de jun de 2018). *Bitcoins News.* Obtenido de Bitcoinist is a Bitcoin news portal providing breaking news about decentralized digital money, blockchain technology and Fintech: https://bitcoinist.com/breaking-down-the-scalability-trilemma/

Bitfury. (10 de 03 de 2020). *Improving the security of a government land registry.* Obtenido de https://exonum.com/story-georgia

Buldas, A., Kroonmaa, A., & Laanoja, R. (10 de 2013). *Keyless Signatures' Infrastructure:.* Obtenido de Guardtime AS - Tallinn University of Technology: https://eprint.iacr.org/2013/834.pdf

Casa Rosada Presidencia. (22 de 02 de 2016). *El Gobierno presentó un Plan de Modernización de la Argentina.* Obtenido de https://www.casarosada.gob.ar/slider-principal/35580-presentan-un-plan-de-modernizacion-de-la-argentina

Chinchilla, C. (17 de 06 de 2019). *A Next-Generation Smart Contract and Decentralized Application Platform.* Obtenido de https://github.com/ethereum/wiki/wiki/White-Paper

Chowdhry, B. (06 de 11 de 2015). *HUFFPOST.* Obtenido de I (Shall Happily) Accept the 2016 Nobel Prize in Economics on Behalf of Satoshi Nakamoto: https://www.huffingtonpost.com/bhagwan-chowdry/i-shall-happily-accept-th_b_8462028.html

Colegio Público de Abogados de la Capital Federal. (2020). *Guía "Acerca del punto 11 de la Acordada 4/2020".* http://www.cpacf.org.ar/files/acordadas/Punto%2011%20Acordada%20CSJN%204-2020.pdf.

Curran, B. (25 de 09 de 2019). *What is Ethereum? Beginner's Guide to This Decentralized Computing Platform.* Obtenido de BLOCKONOMI Guide: https://blockonomi.com/ethereum-guide/

Danish Maritime Authority . (21 de 04 de 2020). *Blue Denmark.* Obtenido de https://www.dma.dk/Vaekst/MaritimErhvervspolitik/DetBlaaDanmark/Sider/default.aspx

Danish Maritime Authority. (18 de 05 de 2018). *Blockchain technology set to renew and ease ship registration.* Obtenido de Blockchain technology set to renew and ease ship registration

Douceur, J. R. (2002). The Sybil Attack. En P. Druschel, M. F. Kaashoek, & A. I. Rowstron, *Revised Papers from the First International Workshop on Peer-to-Peer Systems* (págs. 251-260). London: Springer-Verlag.

e-Estomia. (13 de 04 de 2020). *Blockchain KSI ® en Estonia.* Obtenido de https://e-estonia.com/solutions/security-and-safety/ksi-blockchain

eEstonia. (Marzo 2020). *KSI ® blockchain in Estonia.* Obtenido de https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf

Eileen Gardiner, R. G. (2015). *The Digital Humanities: A Primer for Students and Scholars. . .* Cambridge University Press.

Gartner. (08 de 10 de 2019). *Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact.* Obtenido de https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact

Guardtime. (13 de 04 de 2020). *Guardtime Homepage .* Obtenido de https://guardtime.com/technology

Guardtime. (20 de 04 de 2020). *Guardtime Homepage.* Obtenido de https://guardtime.com/technology

Guzmán, S. S. (06 de 03 de 2020). *Registro panameño a la vanguardia tecnológica para una mayor eficiencia.* Obtenido de HUB: https://www.hub.com.pa/registro-panameno-a-la-vanguardia-tecnologica-para-una-mayor-eficiencia/

Hyperledger. (08 de 2018). *An Introduction to Hyperledger.* Obtenido de The Hyperledger White Paper Working Group : https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf

Hyperledger Avalon. (03 de 10 de 2019). *https://www.hyperledger.org/blog/2019/10/03/introducing-hyperledger-avalon.* Obtenido de https://github.com/hyperledger/avalon .

International Registries. (2014). *a history of International Registries Inc.* Obtenido de http://www.claymaitland.com/wp-content/uploads/2009/08/A-History-of-International-Registries-Inc.pdf

Jentzsch, C. (24 de 08 de 2016). *The History of the DAO and Lessons Learned.* Obtenido de slock.it Blog: https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5

jpmorganchase/cuorum. (17 de 08 de 2018). *Quorum Overview.* Obtenido de GitHub: https://github.com/jpmorganchase/quorum/wiki/Quorum-Overview

Koonce, L. (18 de Feb de 2016). *Transferencias de Activos y Fichas Digitales (Por qué la cadena de bloques es importante para las artes, Parte 2).* Obtenido de https://medium.com/creativeblockchain/transfers-of-digital-assets-and-tokens-why-blockchain-matters-to-the-arts-part-2-5e014a0479bd

Ledger Insights. (2019). *UK Land Registry selects Corda for blockchain.* Obtenido de https://www.ledgerinsights.com/uk-land-registry-corda-blockchain-property/

Liberian Registry. (06 de 03 de 2020). *History Of Liberia's Program.* Obtenido de https://www.liscr.com/history-liberia%E2%80%99s-maritime-program

Liberian registry. (07 de 03 de 2020). *Liberian Registry.* Obtenido de https://www.liscr.com/sites/default/files/Vessel%20Registration%20in%20Liberia%20FLOWCHART%20Rev.%202016-08.pdf

Litan, Avivah. (08 de 10 de 2019). *El ciclo Hype de Gartner 2019 muestra que la mayoría de las tecnologías Blockchain aún están a cinco o 10 años de distancia del impacto transformador.* Obtenido de https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact

Maikro. (04 de 12 de 2019). *Bite-Sized Entry #5: International E-Registry of Ships (IERS).* Obtenido de An overview of the digital blockchain-based ship registration and renewal process: https://medium.com/perlin-network/bite-sized-entry-5-international-e-registry-of-ships-iers-f486286f5d2

Maritime and Port Authority of Singapore. (05 de 09 de 2019). *China Maritime Safety Administration and Maritime and Port Authority of Singapore ink MOU to Promote Bilateral Use and Recognition of Electronic Certificates in Shipping.* Obtenido de https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/detail/7c5bd100-98df-4a33-9d36-b7a5dd633cbf

medium.com. (09 de 03 de 2020). *International E-Registry of Ships (IERS).* Obtenido de https://medium.com/perlin-network/bite-sized-entry-5-international-e-registry-of-ships-iers-f486286f5d2

Methods. (13 de 09 de 2018). *Digital Street: HM Land Registry has selected to partner with Methods.* Obtenido de https://methods.co.uk/blog/hm-land-registry-have-selected-to-partner-with-methods/

MinEduc. (29 de diciembre de 2011). *Infoleg.* Obtenido de Resolución 160/11 Ministerio de Educación: http://servicios.infoleg.gob.ar/infolegInternet/anexos/190000-194999/192733/texact.htm

Ministerio de Modernización. (2018). *XVI Congreso Int. Inov. Tecno. Informática Bs. As. – Sept 2018.* Obtenido de https://slideplayer.es/slide/14904622/

Ministerio de Modernización. (2018). *XVI Congreso Int. Inov. Tecno. Informática Bs. As. – Sept 2018.* Obtenido de https://slideplayer.es/slide/14904622/91/images/18/GDE+es+un+Ecosistema+propietario+de+Arquitectura+Open+Source.jpg

Ministerio de Modernización. (25 de 04 de 2019 01:25). *Interoperar.* Obtenido de https://repositorio.modernizacion.gob.ar/pages/viewpage.action?pageId=52924435

Mora, S. J. (31/12/2013). Documento digital, firma electrónica y digital. *La Ley - Enfoques 2014 (febrero)*, 502 .

Nakamoto, S. (31 de 10 de 2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Obtenido de https://bitcoin.org/bitcoin.pdf

Nikkei Inc. (14 de 06 de 2017). *Asian review.* Obtenido de https://asia.nikkei.com/Markets/Property/Japan-to-tidy-up-scattered-property-records

Official Guide to Ship & Yacht Registries ("OGSR"). (06 de 03 de 2020). *Official Guide to Ship & Yacht Registries*. Obtenido de Marine Money : https://www.guidetoshipregistries.com

Oram, A. (2001). *Peer-to-Peer: Harnessing the Power of Disruptive Technologies.* Sebastopol, CA, USA: O'Reilly & Associates, Inc.

PDMS Ltd. (s.f.). *Bahamas Maritime Authority.* Obtenido de https://www.pdmsregistrysolutions.com/bahamas-maritime-authority/

Pérez, I. (22 de 10 de 2016). *Corda, plataforma nativa del R3CEV, será de código abierto.* Obtenido de Criptonoticias: https://medium.com/poa-network/introducing-oracles-network-864d1d7e37e2

Perez, Isabel. (10 de 03 de 2020). *Criptonoticias.* Obtenido de Suecia concluye con éxito prueba de registro de propiedad basado en blockchain: https://www.criptonoticias.com/aplicaciones/suecia-concluye-exito-prueba-registro-propiedad-basado-blockchain/

Pérez, J. L. (2016). *La economía de blockchain: Los modelos de negocio de la nueva web.* España: kolokium.

Property Guru. (26 de 09 de 2019). *Japan shows yen for blockchain innovation.* Obtenido de https://www.asiapropertyawards.com/japan-shows-yen-for-blockchain-innovation/

Quorum Whitepape. (21 de 11 de 2016). *GitHub.* Obtenido de jpmorganchase/quorum-docs: https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.1.pdf

Revista Marítima - RM Fowarding. (26 de 10 de 2019). *RM Fowarding.* Obtenido de Registro de buques. Probarán sistema electrónico: http://rm-forwarding.com/2019/10/26/registro-de-buques-probaran-sistema-electronico/

Ria. (09 de 07 de 2019). *Data Exchange Layer X-tee .* Obtenido de https://www.ria.ee/en/state-information-system/x-tee.html

Rodriguez, N. (20 de 09 de 2018). *Algoritmos de consenso: la raíz de la tecnología blockchain101blockchain.* Obtenido de 101 Blockchains: https://101blockchains.com/es/algoritmos-de-consenso-blockchain/

Ryan. (27 de 05 de 2017.). *Digital Cash.* Obtenido de School of Computer Science, University of Birmingham: http://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/DigitalCash.html

Safety4sea. (11 de 05 de 2018). *Denmark to reduce administrative burdens in maritime with blockchain.* Obtenido de https://safety4sea.com/denmark-to-reduce-administrative-burdens-in-maritime-with-blockchain/

Ship Technology Global. (15 de 10 de 2019). *SSA, ICC and Perlin partner to build ship registration system.* Obtenido de https://www.ship-technology.com/news/ssa-icc-perlin-ship-registration/

SmartDegrees News. (10 de 03 de 2020). *Georgia crea un registro de la propiedad con blockchain.* Obtenido de https://www.smartdegrees.es/georgia-crea-un-registro-de-la-propiedad-con-blockchain/

Steinmetz, R., & Wehrle, K. (2005). What Is This “Peer-to-Peer” About?. En *Peer-to-Peer Systems and Applications.* (págs. 9-16.). Springer Berlin Heidelberg.

Tramites a distancia. (2020). Obtenido de https://tramitesadistancia.gob.ar/tramitesadistancia/dctramite;idTipoTramite=4340

Trilema. (s.f.). *Wikipedia.* Obtenido de https://en.wikipedia.org/wiki/Trilemma

Trustnodes. (23 de 11 de 2019). *¿El genio de Estonia, Satoshi Nakamoto?* Obtenido de https://www.trustnodes.com/2019/11/23/estonias-genius-satoshi-nakamoto

UNCTAD . (10 de Deceber de 2019). *United Nations Conference on Trade and Development*. Obtenido de UNCTADstat. e-Handbook of Statictis2019: https://unctadstat.unctad.org.

Viswanathan, S., & Shah, A. (20 de 10 de 2018). *The Scalability Trilemma in Blockchain.* Obtenido de NeonVest: https://medium.com/@aakash_13214/the-scalability-trilemma-in-blockchain-75fb57f646df

Vitalik Buterin. (2014). *Ethereum White Paper.* Obtenido de https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Wallece, B. (2011). The Rise and Fall of Bitcoin. *Wired*.

Wikipedia. (20 de 03 de 2019). *Peer-to-peer.* Obtenido de https://es.wikipedia.org/wiki/Peer-to-peer

Wikipedia. (11 de 03 de 2020). *Árbol de Merkle.* Obtenido de https://es.wikipedia.org/wiki/%C3%81rbol_de_Merkle

Wikipedia. (11 de 03 de 2020). *Cryptographic hash function.* Obtenido de https://en.wikipedia.org/wiki/Cryptographic_hash_function

Wikipedia. (03 de 11 de 2020). *Función Hash.* Obtenido de https://es.wikipedia.org/wiki/Funci%C3%B3n_hash

Wikipedia. (06 de 03 de 2020). *Historia de Liberia.* Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Liberia

Wikipedia. (17 de 03 de 2020). *Hyperledger.* Obtenido de https://es.wikipedia.org/wiki/Hyperledger

Wikipedia. (08 de 03 de 2020). *International Registries, Inc. (IRI)*. Obtenido de https://en.wikipedia.org/wiki/International_Registries

Wikipedia. (17 de 03 de 2020). *Satoshi Nakamoto.* Obtenido de https://es.wikipedia.org/wiki/Satoshi_Nakamoto

Wikipedia. (s.f.). *Activo digital.* Obtenido de https://es.wikipedia.org/wiki/Activo_digital

Zhang, J. (18 de 05 de 2018). *Consensus Algorithms: PoA, IBFT or Raft?* Obtenido de https://kaleido.io/consensus-algorithms-poa-ibft-or-raft/

QUAERERE VERUM
Universidad de
SanAndrés