El futuro digital es de todos

Gobierno de Colombia
MinTIC

DLT/BLOCKCHAIN

Borrador - Guía para el uso y la implementación de tecnología de registros distribuidos (DLT/Blockchain) en el sector público

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Economía Digital
Dirección de Gobierno Digital

Equipo de trabajo
Karen Abudinen Abuchaibe - Ministra de Tecnologías de la Información y las Comunicaciones
German Rueda - Viceministro de Economía Digital
Alexander Castiblanco - Asesor
Aura Cifuentes - Directora de Gobierno Digital
Juan Carlos Noriega – Coordinación del Grupo Interno de Política
Juan Pablo Salazar – Coordinación del Grupo Interno de Política
Santiago Ortega – Coordinación del Grupo Interno de Política
Luisa Fernanda Medina – Subdirección de fortalecimiento de capacidades públicas digitales
Carlos Julio León – Subdirección de fortalecimiento de capacidades públicas digitales

Director ejecutivo del Centro de Bioinformática y Biología Computacional –BIOS–
Dany León Molina Orrego

Desarrollo técnico del documento
Jorge Cifuentes

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Versión	Observaciones
Versión 1 Diciembre 2018	Guía para el uso y la implementación de tecnología de registros distribuidos (DLT/Blockchain) en el sector público
Versión 2 Agosto 2020	Ajustes de estilo y forma

Tabla de contenido

Lista de Figuras

Lista de Tablas

1. Introducción

La presente guía comprende una contextualización de DLT (Tecnología de Registros Distribuidos, en inglés Distributed Ledger Technology); conceptos y usos, cuáles son las potencialidades y limitaciones de la tecnología, qué tipos de DLT existen, las aplicaciones existentes relacionando su impacto social y económico, y por último se muestra la relación del DLT con la generación de políticas públicas y sus posibilidades de uso a nivel gubernamental.

Este documento tiene como objetivo suministrar al lector un conocimiento básico de esta tecnología y proporcionarle un contexto de su uso, para así promover el crecimiento de iniciativas que concreten proyectos basados en DLT, orientados a facilitar la interacción del gobierno y los ciudadanos, generando valor social y económico. La implementación de esta guía permitirá de igual forma a las entidades públicas establecer frente a un referente, su nivel de alistamiento para implementar servicios basados en DLT. Finalmente, la guía también permitirá establecer recomendaciones para la formulación de política pública relacionadas con la tecnología DLT.

DLT se le denomina a una tecnología que tiene como objetivo generar un registro distribuido en un ambiente digital interconectado por una red de datos. Las formas cómo se escribe en el registro, cómo se garantiza la autenticidad y cómo se estructura la integridad de la cadena de registros, conllevan a que existan diferentes tipos de DLT, por lo tanto, DLT es una tecnología que posee diferentes formas de implementarse.

DLT se considera una innovación disruptiva en la forma en que se pueden realizar transacciones en redes de comunicación, mayormente en la web, el mayor cambio proporcionado por esta tecnología es una modificación cultural; la cual logra dos grandes transformaciones: la primera consiste en otorgar confianza a un registro digital, en mayor o igual grado que a un documento físico, y la segunda radica en que la validez del documento no es otorgada por una autoridad central y en cambio se acepta que la red, de forma democrática, sea la que otorgue y garantice la autenticidad, la integridad y por ende la validez del documento electrónico.

La clave en DLT/Blockchain es generar “Confianza” en las transacciones que se realicen en la red, al punto que no se requieran ni documentos físicos (Papeles) o entidades centralizadas (Bancos o Notarios) para poseer un título que represente valor social o económico.

En la Figura 1 DLT/Blockchain es Confianza en lo Digital se resalta un concepto central, DLT es útil si se desea generar un aplicativo mediante el cual se va a confiar en lo digital, lo válido es la evidencia (valor, identificador) que se encuentre en el registro distribuido, construido mediante una cadena de bloques.

Figura 1 DLT/Blockchain es Confianza en lo Digital

Para generar confianza en los usuarios, DLT se ocupa de dos aspectos importantes uno es la validez de la información existente en los registros y el otro cómo se otorga la autoridad de escritura sobre los registros (quién, cómo y cuándo puede escribir un registro). El primer aspecto se gestiona mediante métodos criptográficos y el segundo estableciendo formas de conceso en el que los tiempos y la posibilidad de escribir estén distribuidos en los nodos que conforman la red. En la Figura 2 se ilustra los ejes generadores de confianza en DLT.

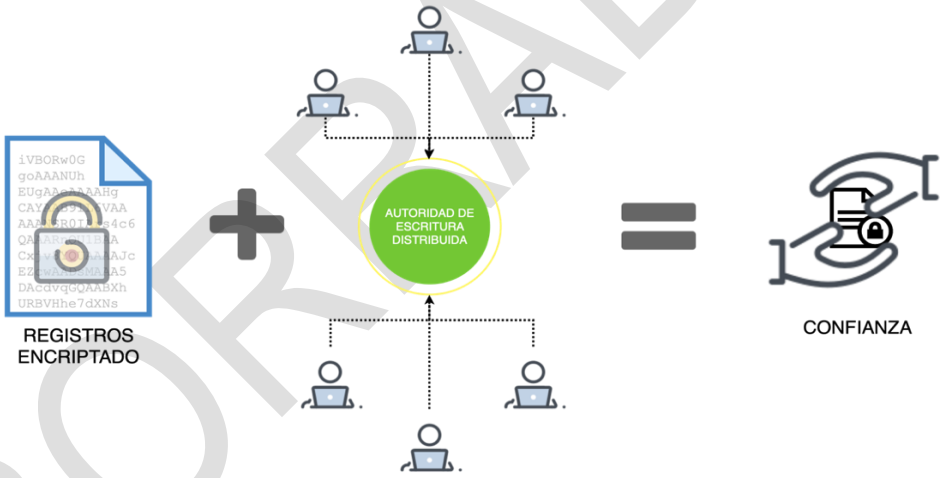

Figura 2 Ejes generadores de confianza DLT

Las características de confidencialidad, autenticidad, integridad, trazabilidad y disponibilidad (hacia abajo aumenta la complejidad tecnológica) que se podrían garantizar a través de la tecnología DLT. Hoy en día ya se utilizan otro tipo de tecnologías y técnicas para garantizar por separado cada una de estas características, en especial las tres primeras, las cuales seguramente muchas entidades ya han trabajado. Sin embargo, no se cuenta con una tecnología que las pueda garantizar todas, como DLT, y que a su vez a través de la validación de un registro genere confianza como si se tratara de un documento físico firmado por un notario.

2. Estado del arte

En este capítulo encontraremos diferentes aplicaciones de las tecnologías DLT/Blockchain; en la actualidad, se presentan diferentes entornos o escenarios donde se han hecho desarrollos exitosos. Cada caso presentado muestra un factor relevante en la implementación, demostrando las ventajas y limitaciones de esta tecnología emergente.

Los países miembros y socios de la OCDE (Organización para la Cooperación y el Desarrollo Económico) están definiendo un conjunto de directrices para el uso de tecnologías emergentes (Inteligencia Artificial y Blockchain) en el sector público. Bajo esta perspectiva establecieron un grupo temático que busca comprender mejor las implicaciones, los requisitos y los impactos del uso de tecnologías emergentes (TE) para fomentar la transformación digital del sector público. Los países que participan en dicho Grupo Temático son: Canadá, México, Panamá, Colombia, Chile, Argentina, Uruguay, Portugal, Reino Unido, Países Bajos, Italia, Finlandia, Estonia, Letonia y Eslovenia.

El grupo estableció la necesidad de mapear el uso actual de TE e identificó que los países participantes están probando soluciones de Blockchain en varias áreas de interés del sector público, como se describe en el borrador del documento "Estado del arte en tecnologías emergentes en el sector público" de la OCDE, y las cuales se enunciarán a continuación:

Tabla 1 Uso de soluciones Blockchain en los países miembros del grupo temático de TE de la OECD

SECTOR	USO DE SOLUCIONES BLOCKCHAIN
Criptomonedas	Asegurar la protección de los consumidores que invierten en criptomonedas.
Contratación pública (subvenciones)	Publicación proactiva de subvenciones y datos de contribución en tiempo real (Ethereum Blockchain).
Gestión de emergencias	Mejorar la gestión de riesgos de emergencias.
Autenticación ciudadana	Asegurar la autenticidad del documento y para la autenticación ciudadana.
Impuesto sobre la nómina y contrato laboral	Desarrollar transacciones inteligentes y usar contratos inteligentes como contratos de trabajo.
Seguridad cibernética	Herramienta de evaluación de riesgos que estará disponible para todas las entidades de la administración pública para evaluar su nivel de exposición a amenazas cibernéticas.

Fuente: Grupo Temático de TE de la OCDE "Estado del arte en tecnologías emergentes en el sector público"

Para iniciar la discusión sobre el estado del arte de las DLT se debe precisar que este término inició su diseminación en el sector tecnológico luego de la aparición de Blockchain (ITU-T Focus Group Digital Financial Services, 2017), el cual a su vez nace con el lanzamiento del documento "Bitcoin: A Peer-to-Peer Electronic Cash System" que se publicó en el año 2008 bajo el seudónimo de Satoshi Nakamoto (Nakamoto, 2008).

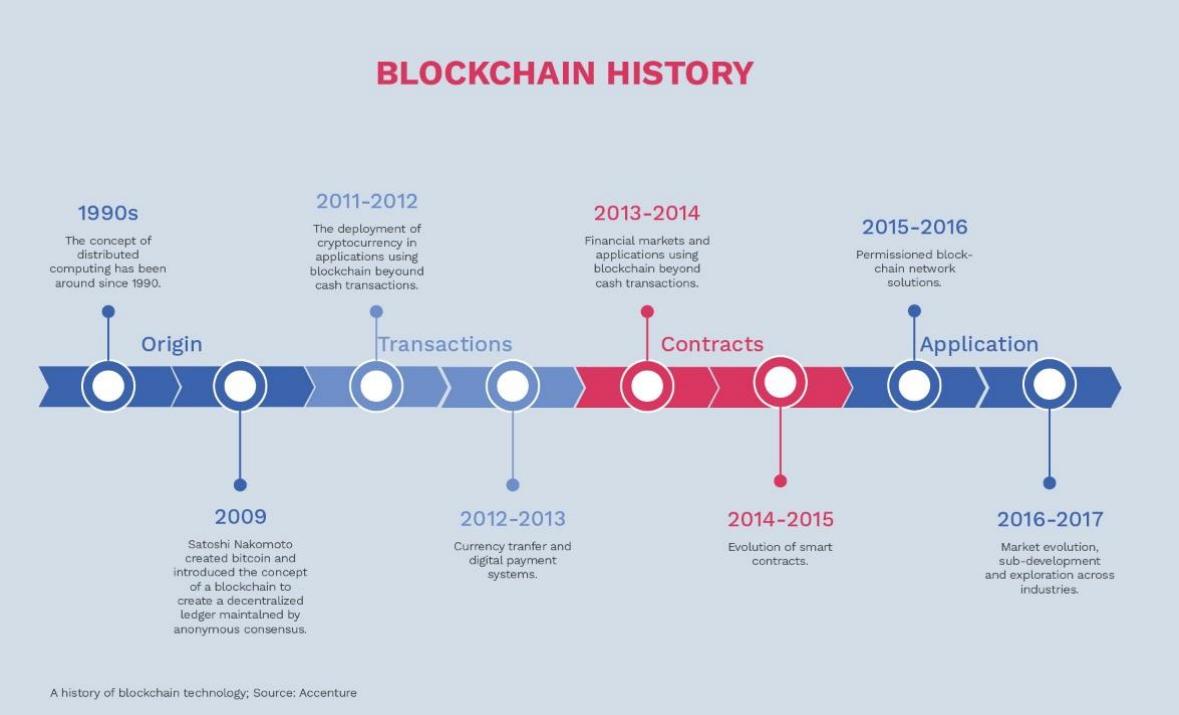

Figura 3 Datos importantes del desarrollo histórico de la tecnología Blockchain

El término DLT es intercambiado con el de Blockchain[1], dado el avance de la terminología y su trascendencia. El Comité Técnico de la ISO encargado de la normalización de esta tecnología (el 307), tiene el mayor avance en el documento "ISO/CD 22739 Blockchain and distributed ledger technologies – Terminology", un documento en construcción que busca establecer una línea de comunicación unificada y general para ayudar en los procesos de discusión posteriores y conducentes a la estandarización (International Organization for Standardization, 2016).

Nota: Actualmente no existe una norma que permita establecer una línea de definiciones estandarizada, se adoptará la misma estrategia de RAND Corporation en su reporte, y se hará uso del término más amplio "DLT/Blockchain" (RAND Europe, 2017) para hacer referencia a esta tecnología de propósito general, como lo definen Catalini & Gans, 2018.

Lo anterior se puede evidenciar un aspecto fundamental, y es que incluso esta tecnología está siento utilizada para generar un gran número de aplicaciones en diferentes áreas, por ejemplo, en el sector de la tecnología se habla de una Web 3.0 basada en Blockchain tal como se muestra en la siguiente imagen:

[1] Blockchain es el tipo de DLT de mayor adopción

Figura 4 "¿Por qué importa la Web 3.0 y por qué debería saberlo?"
Tomado de https://medium.com/@matteozago.

DIFERENCIA ENTRE BLOCKCHAIN Y DLT

"¿Cuál es la diferencia entre 'blockchain' y una DLT? Es más sencillo de lo que parece. Una 'blockchain', una cadena de bloques, es un tipo de DLT. Es decir, se ha producido un fenómeno frecuente: el éxito de un servicio, producto o aplicación concreta supera tan claramente al 'paraguas' que la engloba que acaba incluso fagocitando su nombre. Pero de

la misma forma que no todas las hojas adhesivas son Post-It, no todas las DLT son 'blockchain[2]*"* Figura 5

Figura 5 Comparación del Blockchain vs. DLT

La alta popularidad de "Blockchain", promovida por el surgimiento y éxito de Bitcoin, generó confusión entre DLT y Blockchain, dado que éste último fue presentado y conocido masivamente mucho antes que el mismo DLT.

Otra diferencia importante, es la diferencia entre Blockchain y las Bases de datos distribuidas. Cuando la gente se refiere a Blockchain, normalmente hacen referencia a un sistema distribuido sin control centralizado, mientras que las bases de datos distribuidas son sistemas distribuidos que tienen una autoridad central (Bach, Mihaljevic, & Zagar, 2018).

Más ejemplos de implementaciones de Blockchain son la mayoría de criptomonedas que se conocen: Bitcoin, Ethereum, Litecoin, entre otras; todas son DLTs de tipo Blockchain.

A continuación, daremos un recorrido de los diferentes factores que muestran el futuro, seguridad, interoperabilidad en las tecnologías DLT/Blockchain. Para ello se contemplan factores como proyección, avance, aplicaciones, evaluación e integración. Los temas tratados a continuación hacen referencia a las limitaciones de las tecnologías DLT/Blockchain y los problemas que contempla la escalabilidad y seguridad.

[2] BBVA, Banco Bilbao Vizcaya Argentaria S.A. 2018 (26-04-2018). ¿Cuál es la diferencia entre una DLT y 'blockchain'? Recuperado de https://www.bbva.com/es/diferencia-dlt-blockchain/

La principal característica diferencial de la tecnología DLT/Blockchain es la garantía de la integridad de los datos que son almacenados (Swan, 2015) (Yli-Huumo, Ko, Choi, & Smolander, 2016) ; sin embargo, actualmente esta tecnología presenta algunos retos.

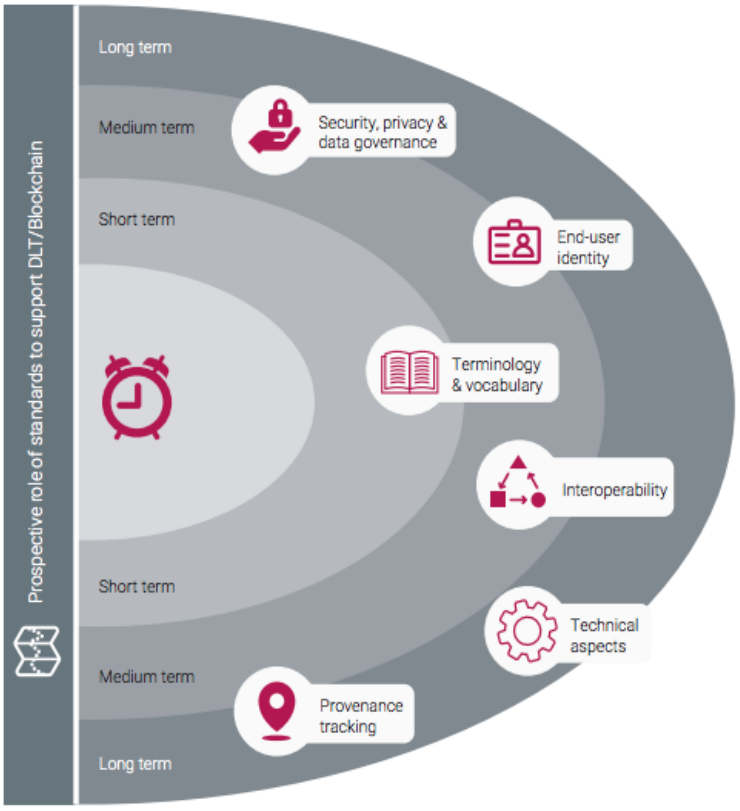

Figura 6 Rol prospectivo de los estándares que soportan la tecnología DLT/Blockchain
Tomado de (Deshpande, Stewart, & Lepeti, 2017)

Con base en la Figura 6, se procede a revisar el estado del arte de la tecnología DLT/Blockchain revisando sus principales aplicaciones y aquellas iniciativas que busquen mitigar o solucionar los principales problemas identificados en su arquitectura y en su puesta en funcionamiento.

2.1. Aplicaciones de DLT para sectores de la economía

El principal uso de DLT/Blockchain a la fecha, sigue siendo la creación e intercambio de criptomonedas; dentro de las cuales Bitcoin se destaca como la aplicación de mayor uso y tamaño basada en esta tecnología. En el documento de la Superintendencia de Industria y

Comercio - Boletín Blockchain, 2018[3], se identificaron los productos y servicios clave que se están desarrollando, los cuales se agrupan en tres áreas: los que crean criptomonedas, los que desarrollan Blockchain en respuesta a las necesidades específicas de las empresas y los que prestan servicios financieros relacionados con Blockchain.

En la Figura 7, se presentan los productos y servicios de la tecnología DLT Blockchain en el mundo; esta gráfica permite visualizar cada clúster de servicios y productos representados por un color: en azul se muestra el de criptomonedas, en rojo las necesidades específicas de las empresas y en amarillo y verde el de servicios financieros (SIC, 2018).

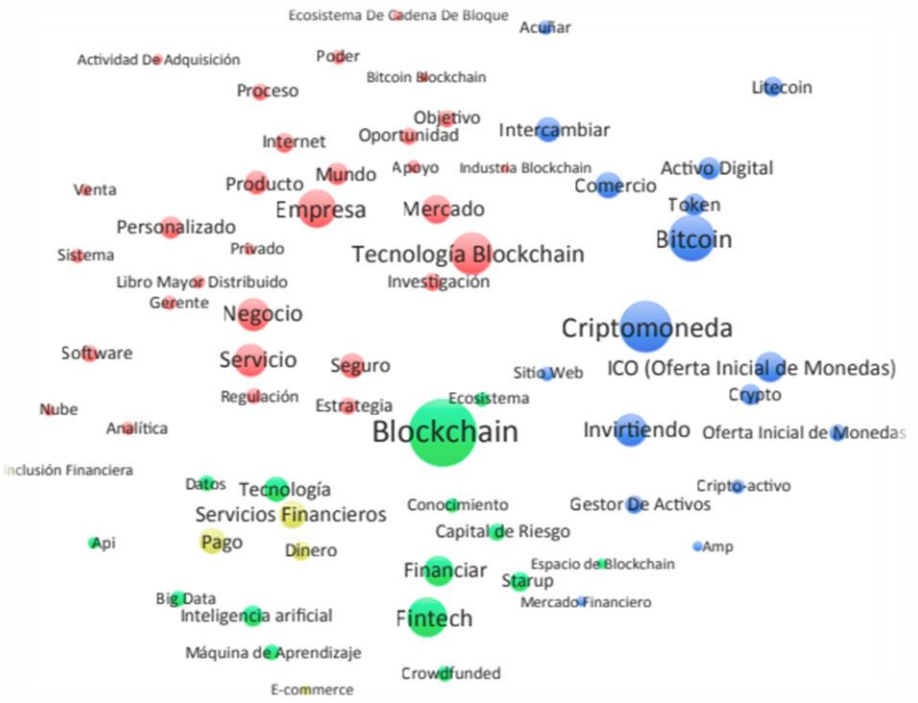

Figura 7 Productos y servicios de la tecnología DLT/Blockchain en el mundo (Google & Bing, 2018)

Con el nacimiento de Ethereum y los "contratos inteligentes" se generaron otro tipo de aplicaciones como las aplicaciones descentralizadas (dApps)[4], las organizaciones descentralizadas autónomas (DAO)[5]; sobre las cuales adicionalmente se han generado

[3] Boletín tecnológico. Superintendencia de industria y comercio (Junio 2018). La revolución de la confianza digital. Tomado de: http://www.sic.gov.co/boletines-tecnologicos/blockchain-la-revolucion-de-la-confianza-digital (Superintendencia de Industria y Comercio, 2018)
[4] Conocidas así por sus siglas en inglés.
[5] Sus siglas en inglés.

numerosas ofertas iniciales de monedas (ICOs)[6] que simulan las ofertas públicas iniciales de empresas tradicionales.

En el caso del sector público, uno de los principales casos de uso es el relacionado con las votaciones, porque permite garantizar la no alteración o manipulación de los resultados mediante un sistema informático; así se enuncia en el artículo "The Future of Democracy: Blockchain Voting" (Osgood, 2016). Adicionalmente, la Oficina de Ciencia de Inglaterra y la OCDE han identificado aquellos casos de uso que podrían tener un mayor impacto en el sector público (Government Office for Science, 2017) (Berryhill, Bourgery, & Hanson, 2018).

Figura 8 Aplicaciones de Blockchain

Colombia no es ajena a esta tendencia, la Alcaldía de Bogotá, en colaboración con investigadores del ViveLabBogotá de la Universidad Nacional, desarrolló una iniciativa para realizar las elecciones de personeros en algunos colegios de la ciudad (Alcaldía de Bogotá, 2018).

Así mismo, ViveLabBogotá con el apoyo del Ministerio TIC, Colciencias, la Agencia Nacional de Tierras (ANT) y UST Global, desarrolló un prototipo Blockchain que permitiría realizar la emisión de los títulos de tierras a cargo de la ANT (El Espectador, 2018).

Adicionalmente, la Universidad Distrital Francisco José de Caldas, desarrolló un documento de investigación para el Centro de Innovación de Gobierno Digital del Ministerio TIC, en función de reducir el riesgo de falsificación de documentos y alteración de credenciales de

[6] Sus siglas en inglés.

usuario a través de su inserción en una Blockchain (Centro de Innovación Pública Digital, 2017).

2.2. Avances en materia de escalabilidad de las DLT

La escalabilidad de las soluciones basadas en DLT/Blockchain es un aspecto a mejorar y depende de manera directa del tipo de algoritmo implementado (al igual que en el caso de la seguridad), puesto que por ejemplo en el caso de los mecanismos de "proof-of-work", además de las limitaciones en el tamaño del bloque (que se relaciona directamente con el número de transacciones), existe un gasto de recursos computacionales que no aportan a la realización de las transacciones sino a la seguridad de la red. Es decir que existe un compromiso entre escalabilidad y seguridad (Kiayias & Pangiotakos, 2015).

Si bien el problema de escalabilidad sigue siendo una línea de investigación abierta, se han planteado soluciones novedosas, como el caso de BigChainDB 2.0, donde se mezclan propiedades de bases de datos (como la posibilidad de hacer consultas, una alta tasa de respuesta y una baja latencia) y la tecnología DLT/Blockchain (Croman, y otros, 2017).

Así mismo, Croman et al. proponen una revisión sistemática de la tecnología DLT/Blockchain para analizar su arquitectura por planos (dividiéndolos en red, consenso, almacenamiento y vistas) y presenta alternativas para solucionar los problemas de escalabilidad en cada uno de estos (BigChain DB GmbH, 2018).

2.3. Evaluaciones sobre la seguridad y confiabilidad de las DLT

La seguridad ha sido uno de los aspectos fundacionales de la tecnología DLT/Blockchain, al ser presentada como uno de sus principales atributos y puntos diferenciales, respecto a los sistemas fundamentados en bases de datos tradicionales.

Figura 9 Finalidad del DLT/Blockchain en materia de seguridad y confianza

Sin embargo, como ha sido referenciado en múltiples fuentes, DLT/Blockchain tiene una principal vulnerabilidad que es el "ataque de mayoría", el cual se da cuando un atacante tiene la posibilidad de controlar o de coordinar al 50% +1 de la capacidad de cómputo de la red (Liao & Lin, 2017) (Mosakheil, 2018). Existen otros tipos de vulnerabilidades asociadas a las criptomonedas las cuales no hacen referencia directa a DLT/Blockchain.

La descentralización por diseño de DLT/Blockchain (y más específicamente de Bitcoin), buscaba minimizar el riesgo de sufrir un "ataque de mayoría", pero al respecto es importante notar que durante los últimos años se ha presentado una centralización paulatina de la red de Bitcoin, lo cual puede llegar a exponer su seguridad (Beikberdi & Song, 2015) y con esto comprometer la reputación de la tecnología de manera general.

Si bien este sigue siendo un frente de investigación abierto, Garay et al. proponen un mecanismo que permite que la nueva red sea tolerante al problema del General Bizantino siempre y cuando se tenga una tercera parte de la red no comprometida (Garay, Kiayias, & Leonardos, 2015).

2.4. Avances en materia de interoperabilidad de las DLT

El estrepitoso avance de las tecnologías DLT/Blockchain ha generado una gran aceptación en diferentes países, empresas y entidades que han empezado a realizar desarrollos en los mismos principios por lo cual se ven tecnologías emergentes adicionales a la tecnología DLT/Blockchain. Por esta razón la interoperabilidad es uno de los principales retos para que esta última sea adoptada de manera masiva, hay diferentes alternativas para atacar este

problema, como lo es el diseño y construcción de un bus de interoperabilidad encargado de alinear todos los sistemas y que facilite la intercomunicación de manera transparente.

En el caso de la tecnología DLT/Blockchain esta aproximación tiene dificultades técnicas bastante altas, por la complejidad que tendrían los contratos inteligentes encargados de actuar como "brokers"[7] entre los diferentes tipos de DLT/Blockchain al intermediar en la ejecución de las transacciones.

Es por esto que la alternativa más viable para garantizar una futura interoperabilidad de la tecnología DLT/Blockchain es la estandarización. Este proceso se podría decir que inició con la creación del Comité Técnico 307 de la ISO en el año 2016, y a la fecha ya cuenta con 39 países miembros y 11 observantes, así como 10 estándares ISO en desarrollo (International Organization for Standardization, 2016). Como se mencionó en los párrafos iniciales de este capítulo, el documento que presenta un mayor avance es el *"ISO/CD 22739 Blockchain and distributed ledger technologies – Terminology".*

Es importante destacar la relevancia de una adecuada intervención por parte de los diferentes actores del ecosistema de DLT/Blockchain, ya que como bien se establece en el reporte preparado por RAND Coorporation para el British Strandars Institution:*"el tiempo correcto para desarrollar e introducir estándares (los cuales se pueden basar en estándares previos) es crítico. Una intervención que ocurra muy temprano puede tener el riesgo de comprometer a las partes interesadas con una solución, que en el largo plazo puede no ser la más eficiente y en el proceso sofocar la innovación. Una estrategia de estándares que suceda muy tarde con respecto a la tecnología tiene el riesgo de perder oportunidades para maximizar los beneficios que la tecnología puede traer"*[8] (RAND Europe, 2017).

3. Identificación de los tipos de DLT

En este capítulo podremos ver las diferentes posibilidades de implementación de acuerdo con los tipos de uso, los tipos de DLT y sus diferencias; también se analizarán los tipos de consensos y los tipos de cadenas como formas para generar modelos de representación.

3.1. Avances en materia de interoperabilidad de las DLT

[7] Según InfoForex (2018), un broker es una persona o una sociedad que se dedica a operar como intermediario, ejecutando las operaciones que le son solicitadas por sus clientes.
[8] Traducción de los autores.

Los tipos de DLT se pueden clasificar en DLT Públicas y DLT Privadas, donde se diferencian según la participación y acceso, entendiendo como participación al ingreso de los usuarios y el acceso y restricciones a los DLT. En cuanto a los accesos podremos definir que se verificaran mediante los consensos de la red, donde el paquete de bloques debe ser verificado según la cadena y ser aceptado por los nodos de la red verificando así la autenticidad del paquete y ser aceptado.

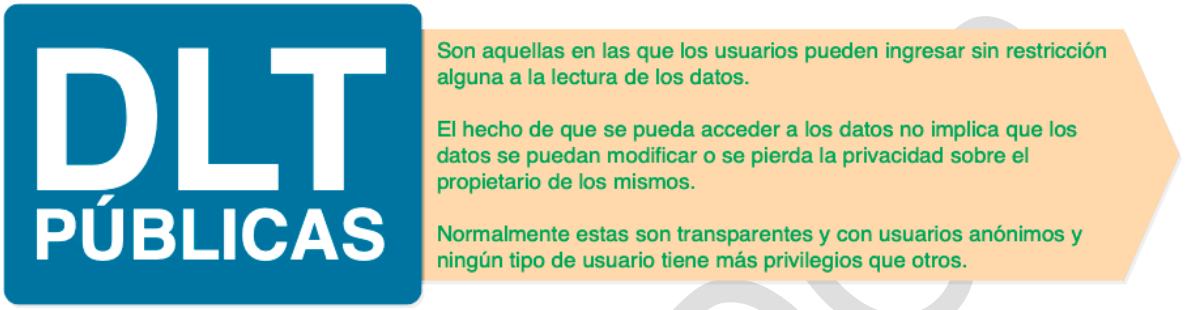

Figura 10 Descripción DLT Públicas

¿Cómo se hace verídica la transacción? Mediante los consensos.

Al azar se escoge un usuario y se determina un nuevo bloque, esto se hace con cada bloque en la cadena, si el bloque es equívoco o fraudulento, los demás participantes pueden bloquearlo o rechazar la conformación del nuevo bloque (Lopez & Unda, 2018).

¿Cuál es la aplicación más conocida de una DLT pública? Bitcoin basada en Blockchain.

Otras formas de DLT públicas se han desarrollado en áreas como transacciones anónimas y contratos inteligente. En esta situación, todos los nodos en todos partes del mundo deben compartir los mismos datos a tiempo que se defienden de ataques de los participantes fraudulentos de la red. (Kyoungmin, Youngin, Mookyu, & Kyungho, 2018).

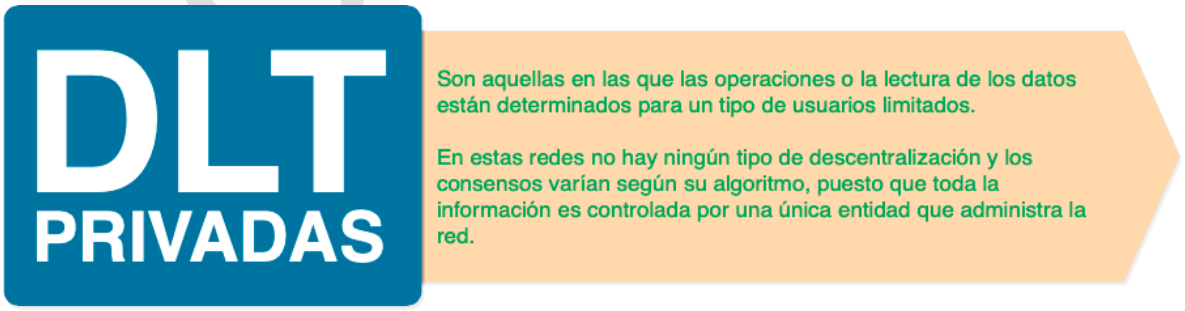

Figura 11 Descripción DLT Privadas

El concepto de DLT es integrador e incorpora los registros distribuidos privados como un tipo de DLT, aun si existe quienes están en desacuerdo con esta inclusión como Marcos Allende López y Vanessa Colina Unda (Lopez & Unda, 2018).

DLT públicas vs. DLT privadas

En la Tabla 2, se presenta un comparativo de las características que se pueden encontrar en las DLT públicas o privadas.

Tabla 2 Comparación entre una DLT Privada y una Pública

CARACTERÍSTICA	DLT PÚBLICA	DLT PRIVADA
Cualquiera puede participar	Sí	No
Los participantes actúan, en general, como nodos	Sí	No
Existe transparencia	Sí	A veces
Hay un único administrador	No	Sí
No hay administradores	Sí	No
Ningún participante tiene más derechos que los demás	Sí	No
Existe recompensa por minado de bloques	A veces	No
Soluciona problemas de falta de confianza	Sí	No
Seguridad basada en protocolos de consenso	Sí	No
Seguridad basada en funciones hash	Sí	A veces
Ejemplos de DLT	Bitcoin Ethereum Litecoin	Hyperledger Corda Quorum

En la Tabla 3, se muestra un ejemplo de una comparación entre una DLT privada y una pública, en esta se puede apreciar que dependiendo de las características ambas, poseen ventajas y desventajas. Desde el punto de vista ambiental es preferible una DLT privada por su bajo consumo de energía y desde la seguridad observada como vulnerabilidad es preferible una DLT pública.

Tabla 3 Características de los tipos de DLT/Blockchain

CARACTERÍSTICA	PÚBLICA	PRIVADA
Número de nodos	Grande (centenas o miles)	Pequeño (unidades o decenas)
Costos infraestructura	Reducidos	Elevados
Costos por transacción	Altos (tokens públicos)	Reducidos (tokens privados)
Vulnerabilidad	Baja (a ataques del 50% +1/ataques de doble gasto)	Alta (a ataques del 50%+1/ataques de doble gasto)
Consumo de energía	Mayor	Menor

3.2. Tipos de consenso

Uno de los elementos constitutivos de una red descentralizada, es la forma en la que esta alcanza el consenso para realizar una determinada acción*, por ejemplo: Insertar una nueva transacción en la base de datos (o cadena de bloques en este caso).

Como se puede encontrar en (Bach, Mihaljevic, & Zagar, 2018), el problema del General Bizantino[9] fue descrito por primera vez en 1982 por Lamport et al, como un problema de confianza en un proceso de comunicaciones, preguntándose sobre cómo podría cada nodo de un sistema estar seguro de que la información que ha recibido es válida.

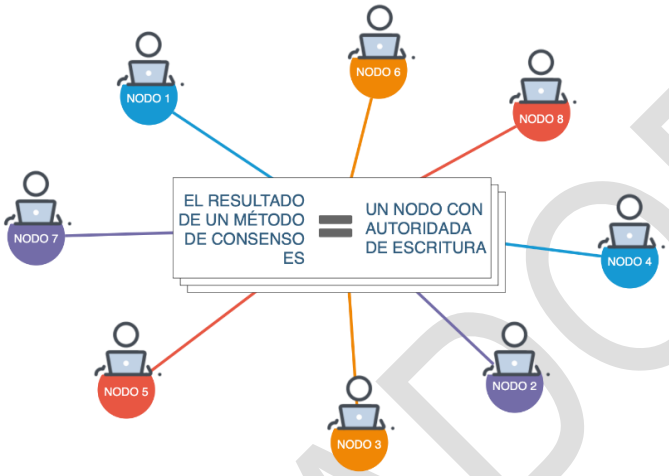

Figura 12 Consenso como método para otorgar autoridad de escritura

Blockchain en su nacimiento (Bitcoin) estableció un mecanismo de consenso que utilizaba la "prueba de trabajo" para garantizar que la red descentralizada era tolerante al problema del General Bizantino.

El caso de NEO, el consenso usado para implementar DLTs/Blockchain públicas, pretende generarse a partir de la "prueba de participación", dando a conocer las implementaciones de DLT/Blockchain que utilizan otros mecanismos para alcanzar el consenso.

Actualmente estos dos tipos de consensos son los más utilizados en la implementación de DLTs/Blockchain públicas, debido a que, dependiendo del diseño de la red, ambos esquemas ofrecen una tolerancia significativa a actores no confiables, haciendo que las soluciones desarrolladas sean tolerantes al problema del General Bizantino (como se muestra en documentos donde se compara el mecanismo compuesto por Nakamoto y aquellos basados en BFT, Blockchain Trader Fund).

[9] En el problema original, la situación que se plantea es la existencia de n generales Bizantinos que están preparando para atacar y para lograr su objetivo, deben hacerlo de manera coordinada (aunque estén fuera de vista los unos de los otros y sólo se pueden comunicar a través de mensajeros que tienen que pasar por el campo enemigo y por lo tanto corren el riesgo de ser interceptados y entregar mensajes incorrectos. Además, existe la posibilidad de que algunos de estos generales sean traidores, y que incluso de manera deliberada envíen un mensaje que no corresponde con la realidad de las cosas.

No obstante, existen otros mecanismos para alcanzar consenso en una red DLT/Blockchain, como es el caso de "prueba de identidad" o "prueba de importancia". El mecanismo de consenso juega un papel primordial sobre la seguridad de DLT/Blockchain, además existe un compromiso entre seguridad y desempeño. En algunas ocasiones mecanismos de consenso que ofrecen una mayor seguridad, también son los que tienen un menor desempeño y afectan la escalabilidad de las soluciones.

A continuación, se mencionan algunas de las principales características de los mecanismos de consenso de las DLTs/Blockchains:

Proof of work (Prueba de trabajo)

El mecanismo de "Prueba de trabajo" basa su popularidad en el hecho de que fue el propuesto para la implementación de la primera DLT/Blockchain (Bitcoin) y en que ha mostrado ser lo suficientemente robusto como para lograr más de 10 años de operación confiable de la red. Se basa en la existencia de un tipo especial de nodo denominado "minero", el cual se encarga de realizar un "trabajo", al resolver un acertijo matemático que busca principalmente comprobar la *disposición y lealtad*[10] del nodo para cooperar con la red.

Nota: Los nodos reciben una compensación por realizar este "trabajo", el cual no está relacionado directamente con la operación o funcionamiento de la red.

Precisamente esta es una de las principales desventajas de este mecanismo, porque malgasta los recursos de la red al poner a algunos nodos a que realicen tareas que no tienen que ver con la operación de esta, sino a comprobar la *lealtad* de los nodos para validar transacciones[11]. Además, como las transacciones deben esperar a que los nodos mineros realicen el "trabajo" asignado, eso representa un problema de escalabilidad, debido a los tiempos de procesamiento de la red.

Para recordar: El estudio realizado por Beikberdi y Song 2015, sobre Bitcoin, donde muestran un patrón de concentración de esta red, que, de mantenerse en el futuro, podría comprometer su seguridad.

[10] En este caso de "proof of work", la disposición y la lealtad de los nodos a trabajar en beneficio de la red está basada en el esfuerzo computacional para resolver los acertijos criptográficos y a recibir un incentivo por este uso de recursos computacionales.

[11] En este punto es importante mencionar que el acertijo matemático es el que no tiene que ver directamente con el funcionamiento de la red, puesto que el proceso de validación de las transacciones obviamente es un proceso fundamental dentro de la DLT/Blockchain.

Proof of stake (Prueba de participación)

Una alternativa a la "Prueba de trabajo" es la denominada "Prueba de participación", por medio de los nodos de antes y del ahora que se muestran en la FFFFF

Figura 13 Antes y ahora de los nodos

Los nodos validadores (bookeepers), se encargan de realizar las respectivas validaciones luego de haberse ganado este derecho, comprando una "participación" dentro del proceso de validación, cumpliendo con tres premisas fundamentales:

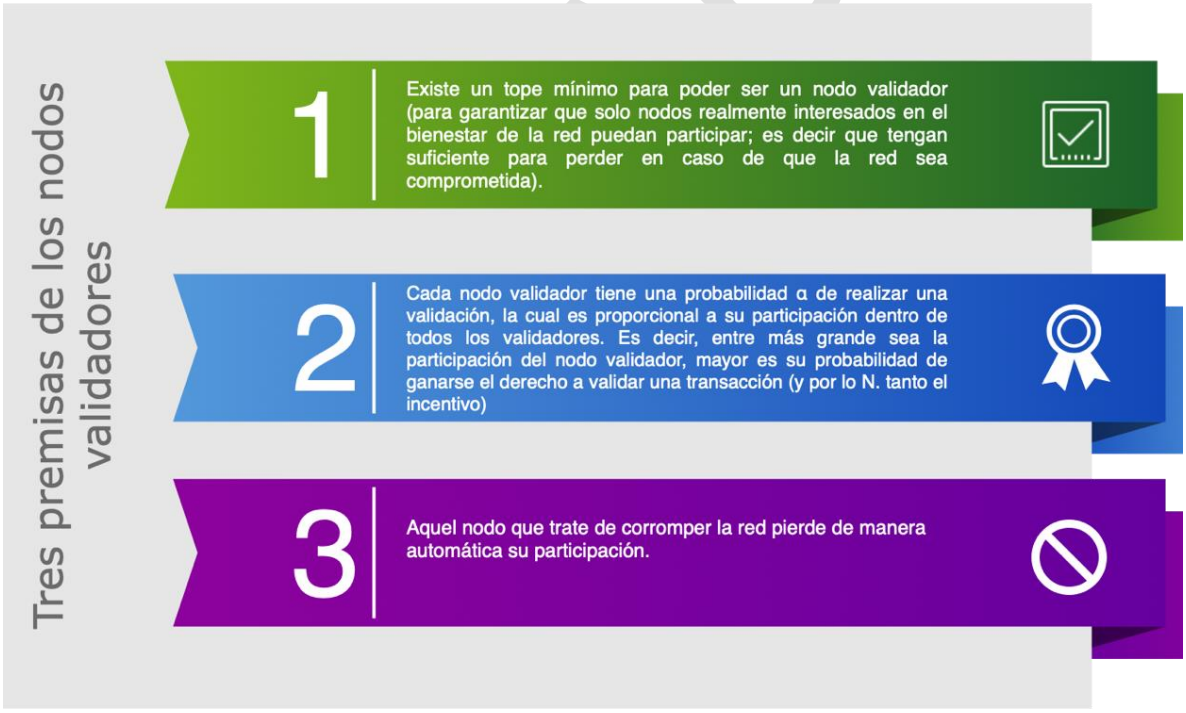

Figura 14 Tres premisas de los nodos validadores

Estas tres características están pensadas para que se pueda maximizar la probabilidad que haya nodos con disposición y lealtad de realizar labores por la red. Los nodos que más validaciones realizarán son aquellos que tienen una mayor participación, y por ende tienen menos incentivos a perderlo todo, realizando una acción corrupta en contra de la red.

Este esquema, al no tener que realizar pruebas criptográficas innecesarias, hace que las redes basadas en este mecanismo de consenso sean mucho más eficientes (y por lo tanto escalables) que aquellas basadas en la prueba de trabajo al no requerir tanto consumo energético ni de hardware especializado.

Importante: En lo teórico, para poder acabar con una red DLT/Blockchain basada en prueba de participación, se requeriría contar con el suficiente dinero como para tener una capacidad considerable de validación en la red y estar dispuesto a perder el dinero.

Proof of burn (Prueba de quemado)

La prueba de quemado puede ser vista como una alternativa a la prueba de trabajo, pero con una mayor eficiencia en materia de consumo energético, puesto que en este caso se realiza una especie de subasta inversa, donde los nodos participantes realizan una oferta de pago por realizar una validación; ésta oferta es proporcional a la probabilidad de obtener la recompensa por dicho trabajo. El nodo ganador paga lo ofertado enviando sus monedas a una cuenta donde solamente se pueden depositar, perdiéndose por siempre. Por eso se denomina "quemar" las monedas, y de ahí el nombre de prueba de quemado (Bach, Mihaljevic, & Zagar, 2018; Slimcoin, 2018).

Este esquema tiene la ventaja que, además de ser más eficiente en términos energéticos, permite cuantificar el valor asignado a garantizar la seguridad de la red de manera explícita, conociendo el balance de la cuenta de quemado, mientras que, en el caso de los mecanismos de prueba de trabajo, los cálculos realizados sobre consumo de energía, son estimados, no valores precisos.

Delegated Proof of stake (Prueba de participación delegada)

La prueba de participación delegada consiste en que no todos los nodos realizan validaciones; en un proceso democrático, se selecciona un número reducido de nodos validadores reales, sobre los cuales se delega esa función.

Para recordar: Al contar con un número menor de nodos de validación, la red funciona de una forma mucho más rápida y eficiente, pero a su vez se tiene una red cada vez más cerrada y más parecida a una red privada (en el sentido de la validación).

Proof of identity (Prueba de identidad)

La forma de participar en el proceso de validación de las transacciones, en el caso de la prueba de identidad, es que, en vez de comprar una participación en la red o realizar un proceso de minado, se aporta una prueba fehaciente de la identidad del responsable del

nodo, permitiendo identificarle de manera fidedigna a fin de hacerlo responsable ante cualquier actividad maliciosa desde el nodo asociado a dicha identidad (Slimcoin, 2018).

Proof of authority (Prueba de autoridad)

Los mecanismos de prueba de autoridad son una familia de algoritmos BFT (Bizantine Fault Tolerant) implementado en redes DLT/Blockchain privadas, su funcionamiento se basa en la existencia de N nodos confiables denominados autoridades donde se asume que al menos $\left(\frac{N}{2}+1\right)$ de estos son honestos. Posteriormente entre estos nodos autoridades se realiza un mecanismo de rotación de minado, para distribuir de manera justa la responsabilidad de creación de bloques entre los nodos (De Angelis, 2018), (Cachin & Vukolic, 2017).

PBFT (Practical Byzantine Fault Tolerant)

El mecanismo de PBFT fue propuesto por Castro & Liskov, 1999 como solución al problema del general bizantino en una red privada y fue utilizado por Hyperledger como algoritmo de consenso. En este esquema existe un nodo líder y otros pares validadores (Cachin & Vukolic, 2017).

Los pares validadores reciben información sobre las transacciones que se deben procesar y proceden a realizar un broadcast a otros pares y al líder. En el momento en el que el número de transacciones alcanza un umbral (denominado batch), el líder ordena las transacciones por el orden de creación y son puestas en un bloque. Posteriormente se ejecutan tres fases:

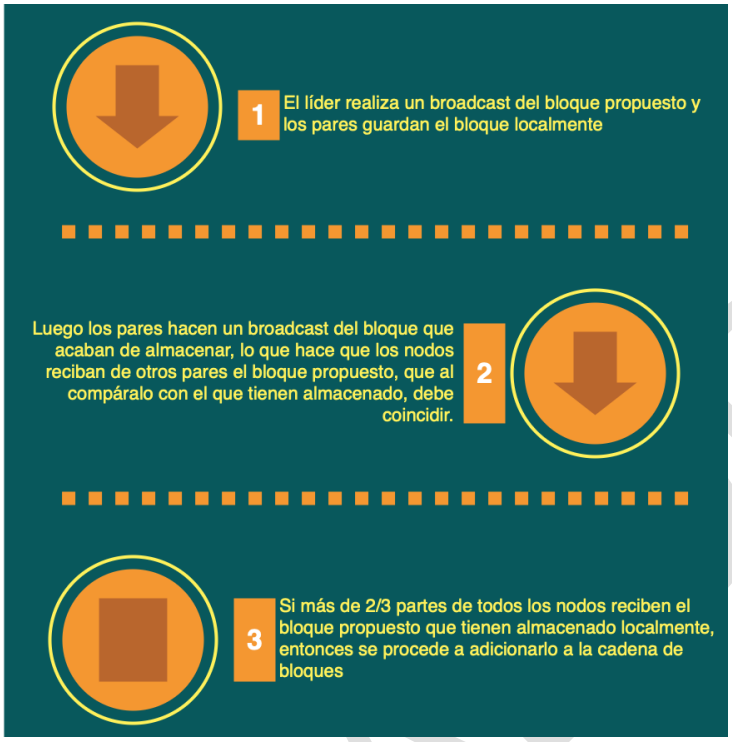

Figura 15 Tres fases de PBFT

Comparación entre Tipos de Consenso

Los tipos de consenso descritos en esta sección se pueden agrupar de dos diferentes maneras: por medio de algoritmos basados en una lotería o mediante el uso de métodos basados en votación; el primero incluye la prueba de tiempo transcurrido y la prueba de trabajo, mientras el segundo la tolerancia de fallas Bizantinas redundantes. Estos enfoques se dirigen a un conjunto de diferentes requisitos de red y modelos de tolerancia a fallas.

Los consensos basados en lotería presentan unas ventajas significativas, ya que pueden escalar gran cantidad de nodos; el ganador, propone un bloque y los transmite al resto de la red para su validación. Los algoritmos generados en estos tipos de consenso en ocasiones conducen a bifurcaciones, cuando dos ganadores proponen un bloque de manera simultánea. Cuando se presentan bifurcaciones, estas deben ser resueltas, lo que implica un tiempo más largo para llevar a término la creación de un bloque en la red.

Por su parte, los consensos basados en votación proporcionan una baja latencia, lo que representa una ventaja; en este caso, cuando la mayoría de los nodos valida una transacción, existe consenso y esto conlleva a la confirmación de las transacciones. La desventaja que presenta este método, radica en el tiempo necesario para alcanzar el consenso ya que los algoritmos basados en votación requieren que los nodos transfieran información a cada uno de los otros nodos de la red.

En la Tabla 4 presentamos una comparación entre los tipos de consenso descritos y el consenso de la prueba de trabajo del cual hace uso Bitcoin.

Tabla 4 Comparación entre tipos de consenso

	ALGORITMOS BASADOS EN UNA LOTERÍA	MÉTODOS BASADOS EN VOTACIÓN	PRUEBA DE TRABAJO ESTÁNDAR (BITCOIN)
Velocidad	Bueno	Bueno	Malo
Escalabilidad	Bueno	Moderado	Bueno
Finalidad	Moderado	Bueno	Malo

3.3. Tipos de cadenas

Los tipos de cadenas en la tecnología DLT, son las formas de generar modelos de representación que permitan crear y almacenar un conjunto de bloques; estableciendo formas de seguir una secuencia en la lectura de los bloques y garantizando la integridad de la información contenida en los mismos.

Blockchain – Cadena de Bloques

Blockchain o cadena de bloques, es una estructura de datos, cuya unidad fundamental son los bloques, los cuales se han creado y organizado por fecha, esta marca de tiempo es inmutable, lo que crea un repositorio digital distribuido, seguro y público; aspectos que facilitan la verificación de los datos en las transacciones[12].

Blockchain es una mezcla de protocolos que se han combinado para lograr un registro de transacciones confiables. Esta confiabilidad se sustenta en el fortalecimiento matemático de la criptografía, específicamente a la creación de algoritmos de clave pública (Algoritmo Diffie-Hellman[13], Árboles de Merkle[14] y Algoritmo RSA[15]).

[12] Esta tecnología puede aplicarse por ejemplo a la industria de los seguros, ya que el tiempo de toma de pólizas, los actores involucrados, el valor de la transacción, y la validez del proceso (Tomado de https://innovate-ieee-org.ezproxy.unal.edu.co/innovation-spotlight/blockchain-framework-insurance-processes-claims/).
[13] Métodos de intercambio de claves en un esquema de alta seguridad
[14] Criptosistema de clave pública
[15] Sistema Criptográfico de clave pública más utilizado, tanto para cifrar como para firmar digitalmente.

Para recordar: La tecnología **Blockchain** es útil para los procesos que requieran **almacenar datos y transacciones donde el tiempo en el que se efectúan es crucial**, con la **garantía de que no se pueden modificar**, ya que es el consenso entre todos los nodos de la red el que permiten almacenar y por ende tener la información replicada, sin tener una entidad que lo certifique. El almacenamiento de la información es distribuido y corresponde a la cadena de bloques, los cuales son transmitidos a redes (peer to peer) punto a punto, o también son lo que se denomina redes de pares.

Nota: La confirmación de los datos se logra por el consenso entre los nodos.

En la Figura 16, se puede identificar el bloque inicial llamado Génesis. Por ejemplo: En el caso de Bitcoin, se considera que el primer bloque lo generó su creador, conocido sólo por su seudónimo, Satoshi Nakamoto.

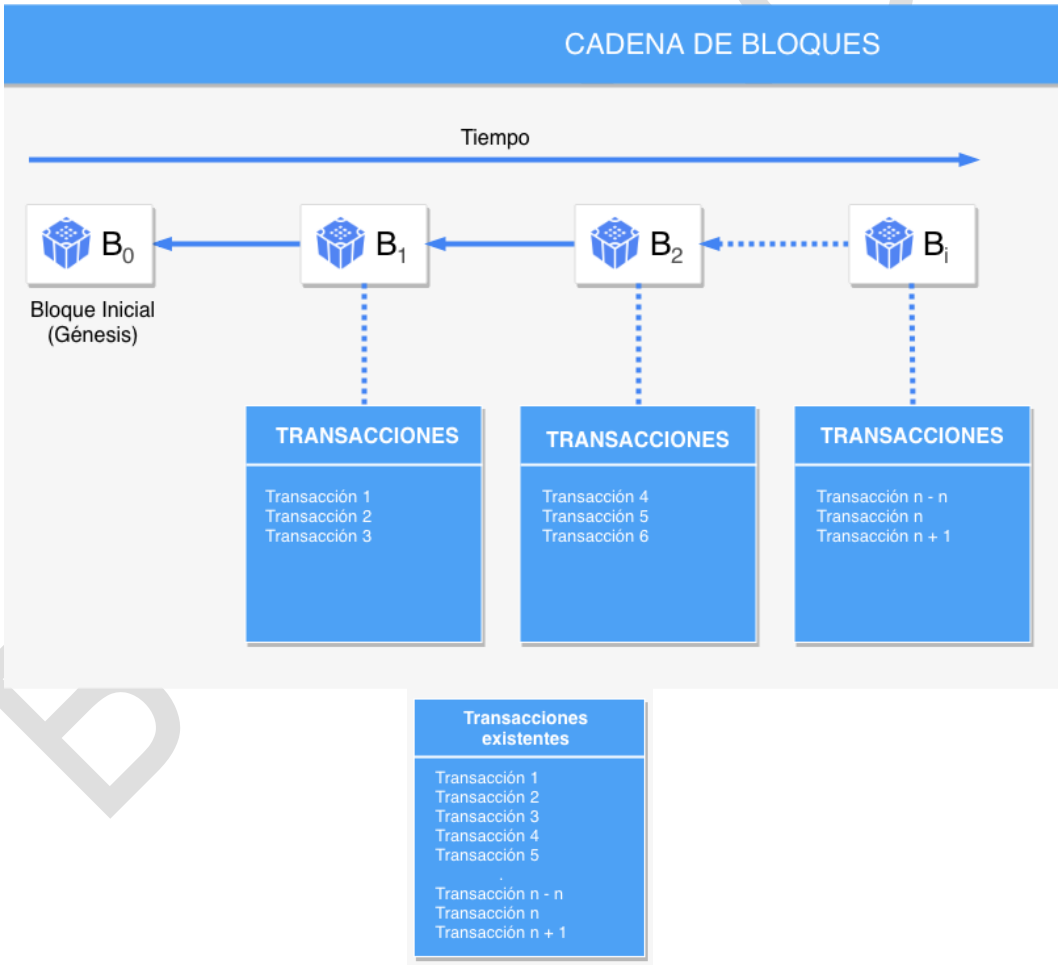

Figura 16 Cadena de Bloques *Tomada de: http://intechractive.com*

Los bloques y transacciones se almacenan utilizando diferentes técnicas criptográficas para garantizar la integridad; el conjunto de todos los bloques y su distribución por toda la red de pares, es denominado el estado actual del sistema que contiene todas las transacciones realizadas hasta el momento y cada par conserva una copia de todos los bloques, que a su vez unen dentro de cada nodo o par utilizando diferentes técnicas criptográficas que permiten garantizar la integridad de la información.

Los bloques están compuestos por tres elementos: Dato, Hash[16] y Código Hash del bloque anterior; cómo se puede ver en la Figura 17, el H( ) fue el Hash definido para bloque Génesis por el creador.

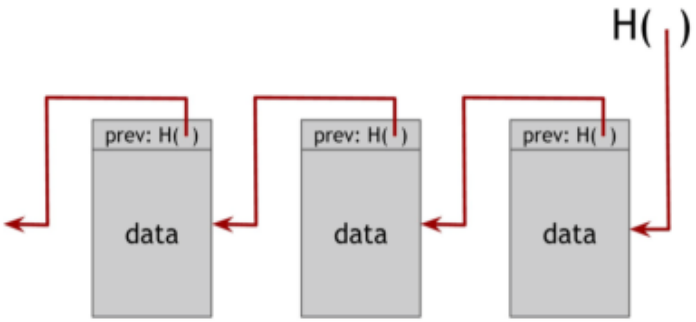

Figura 17 Estructura de una cadena de bloques[17]

Cada bloque de la cadena contiene la información de las transacciones realizadas en un periodo y es en este momento donde se utiliza el algoritmo de árbol de Merkle para representar la cadena.

Nota: El árbol de Merkle es una estructura basada en hash. En la cual se asigna datos a una clave. Los árboles de Merkle se utilizan para verificar datos, son eficientes a la hora de utilizar hashes en lugar de un archivo completo de información.

Por ejemplo: En los portales Etherscan y Etherchain (rastreadores de transacciones Etherium disponibles en https://etherscan.io/ y https://www.etherchain.org/), se pueden identificar la estructura de un bloque de la criptomoneda Ethereum con identificador 6430198 con los siguientes campos:

Heigh	Número del bloque
TimeStamp	Marca tiempo del bloque
Transactions	Operaciones asociadas al bloque

[16] Hash es una función criptográfica, basado en un algoritmo matemático que transforma cualquier bloque de datos en una nueva serie de caracteres, con una longitud fija.
[17] Fuente: Libro "Bitcoin and Cryptocurrency Technologies" de la Universidad de Princenton.

Código Hash del Bloque	
Parent Hash	Código Hash del Bloque anterior
Sha3Uncle	Es una modificación de Ethereum no especificada en Blockchain, una forma de validar un bloque cercano al bloque anterior sin serlo
Mined by	Información del identificador que hizo minería al bloque
Difficulty	Dificultad del proceso, tomando como referencia la latencia y el total de instrucciones.
Total Difficulty	Complejidad total de la cadena
Size	Tamaño del bloque
GAS Used y Gas Limit	Son características particulares del algoritmo Ethereum, empleados para estimar el coste computacional asociado a la validación del bloque
Nonce / Proof of Work Nonce	Número aleatorio usado una sola vez, destinado a la autenticación de transferencia de datos entre dos o más partes.
Block Reward	Recompensa del bloque

En la Figura 18 se evidencia el portal Etherscan y los datos de cadena de bloques, relacionados anteriormente.

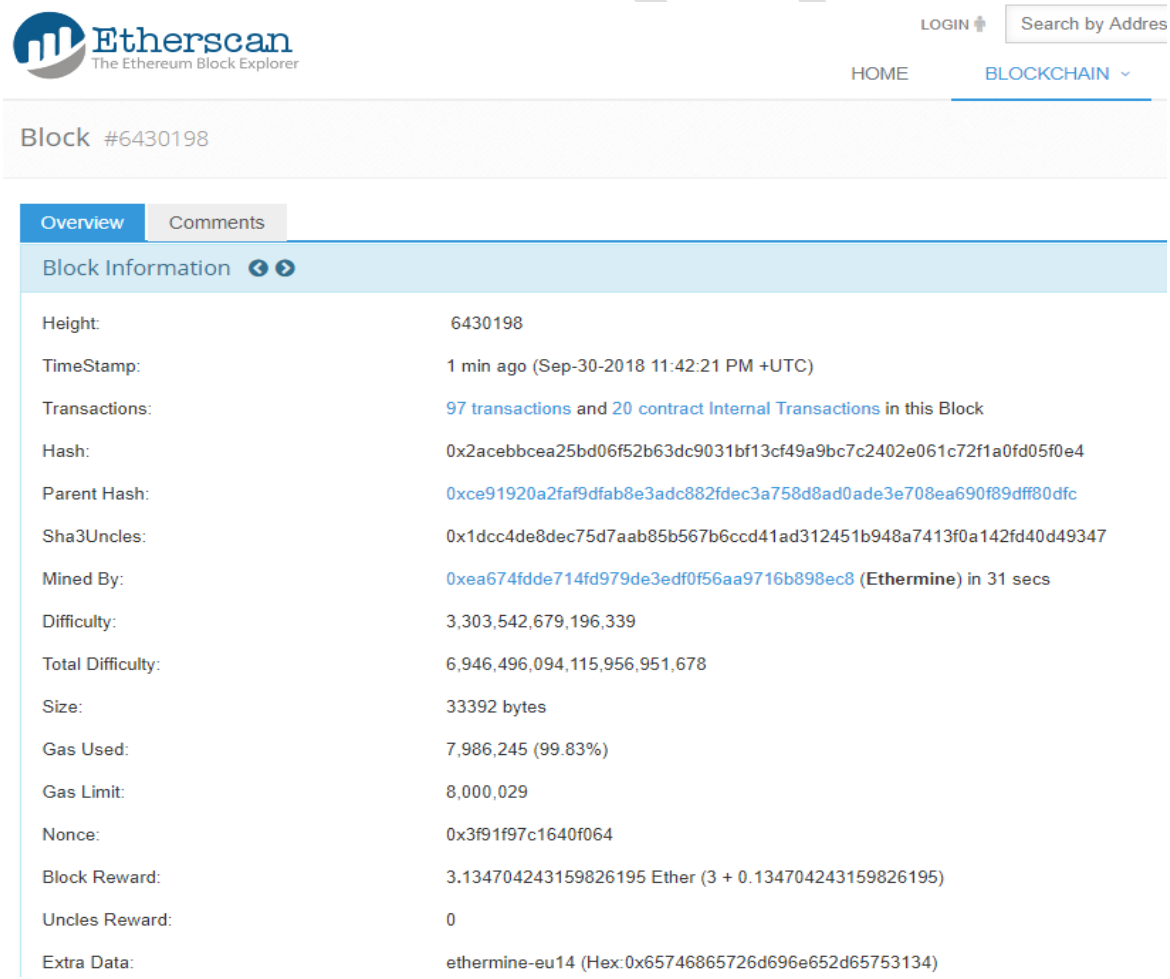

Figura 18 Ejemplo de Información contenida en un bloque Ethereum

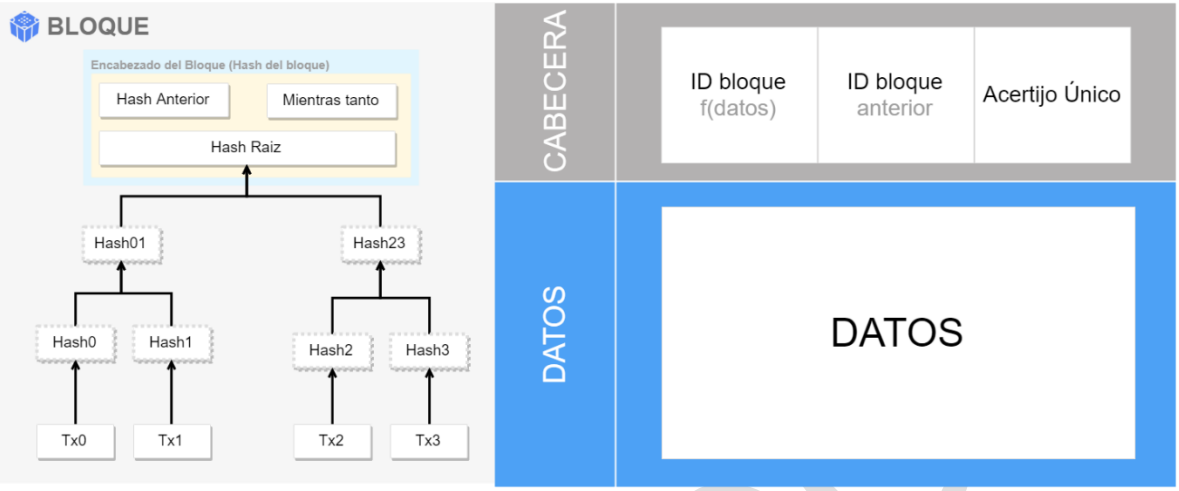

Figura 19 Estructura e información contenida en un bloque de la cadena de bloques (Blockchain) [18].

Directed Acyclic Graphs – Grafos Acíclicos dirigidos

Existen diferentes formas de realizar las transacciones en DLT, en esto vemos que en Blockchain se enlazan por un has mientras que en otra forma se realiza mediante un grafo, son lo grafos acíclicos dirigidos (DAG) elemento fundamental en la arquitectura denominada Tangle. La diferencia más notable entre los dos es que en Blockchain las transacciones se dan en paquetes de bloques criptográficamente unidos, formando una sola cadena que contiene la verdad global; mientras que los DAG usan un grafo en donde una transacción se representa como un nodo en el grafo .

Este modelo DAG fue propuesto por el protocolo IOTA, cuya finalidad es permitir el intercambio de información en dispositivos IOT. Esta arquitectura facilita que no existan comisiones y favorece los micropagos.

[18] Fuente: Bitcoin White Paper.

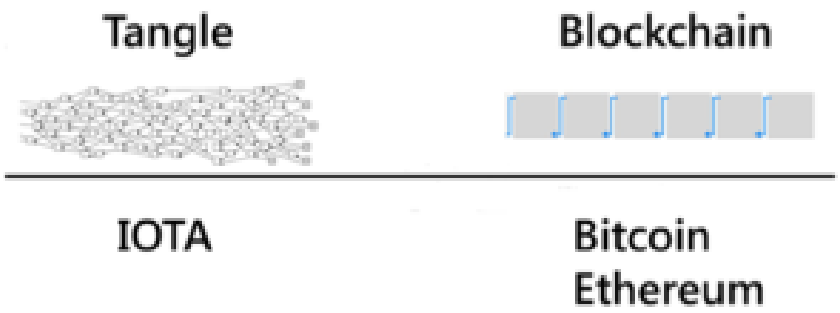

Figura 20 Diferencia entre el modelo Tangle vs Blockchain
Tomado de: https://iotahispano.com/wp-content/uploads/2017/12/TangleVsBoclchain.png

En el anterior gráfico se puede identificar que Tangle (es el libro mayor donde se almacenan las instrucciones). Las transacciones son los nodos del grafo, y se puede aplicar todo el soporte matemático que lo fundamenta entre ellos conceptos como cardinalidad, conexión del grafo, linealidad, camino directo entre dos nodos, costo mínimo, etc.

Funcionamiento del Tangle:[19]

Un grafo está compuesto por nodos, en el caso del protocolo estos nodos representan los sitios que emiten transacciones, pero como la finalidad es la aprobación de las transacciones los nodos deben trabajar en conjunto para aprobarlas. Una transacción se consolida cuando tienen muchas aprobaciones, lo que implica que no entró en conflicto. A continuación, se describen los pasos para que un nodo emita una transacción:

1. El nodo elige otras dos operaciones para aprobar (Pueden coincidir dependiendo del algoritmo).
2. Verifica que las transacciones no entren en conflicto, si esto ocurre no las aprueba.
3. Para que la transacción sea válida debe resolver un rompecabezas criptográfico (desde el punto de vista de la complejidad).

De acuerdo con el procedimiento anterior se puede identificar que la red es asincrónica, cabe señalar también que la Tangle puede contener transacciones contradictorias y que las transacciones transmitidas a la red requieren dos transacciones previas para aprobadas.

En un grafo dirigido la conexión entre los nodos (arcos) tiene asociado un valor, este valor se denomina peso de la transacción y el peso es proporcional a la cantidad de trabajo que el nodo invirtió en ella; los puntajes determinarán que transacciones deberían aprobarse primero. En la siguiente figura se puede identificar las transacciones (recuadros) y en ellos

[19] Tomado como referencia del OTA_Whitepaper_ESP.pdf en el sitio http://www.iotahispano.com

hay dos tipos de números: los números pequeños en la esquina inferior representan el propio peso de las transacciones, mientras que los números en negrita (mayores) son los pesos acumulados.

La puntuación de una transacción es la suma de los pesos propios de todas las transacciones aprobadas por esta transacción más el propio peso de la transacción.

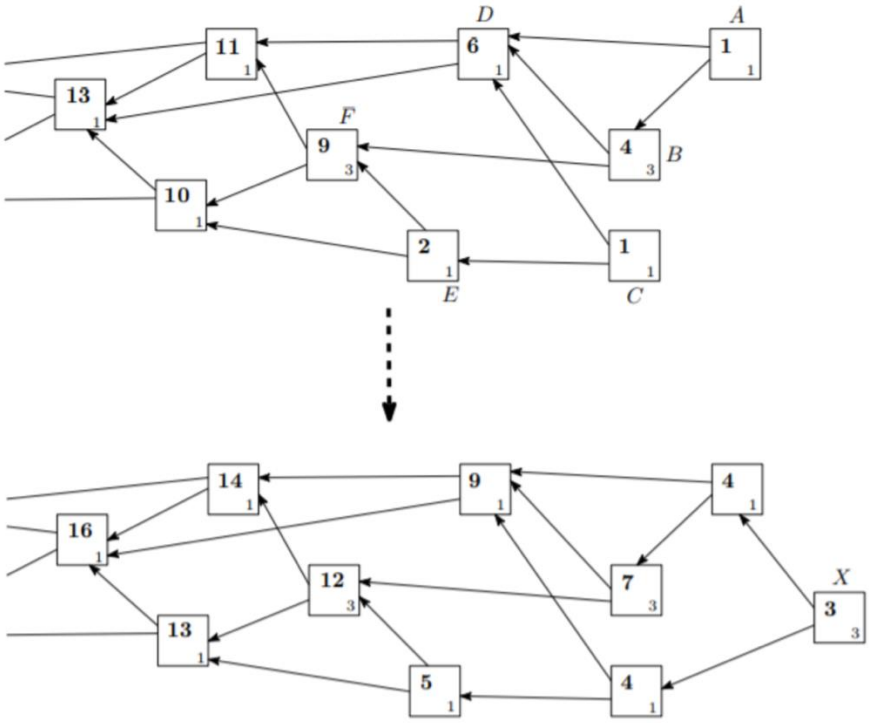

Figura 21 Peso acumulado de las transacciones *Tomado de: https://iota.readme.io/docs/whitepaper Página 6.*

En los algoritmos de aprobación de las transacciones, incorporan variables que dan información general de la estructura del grafo, de acuerdo con la posición de la transacción, estas variables pueden ser:

- Altura (height) como la longitud de la trayectoria más larga orientada a la génesis;
- Profundidad (depth) como la longitud de la trayectoria inversa más larga a alguna transacción sin confirmar (tip)

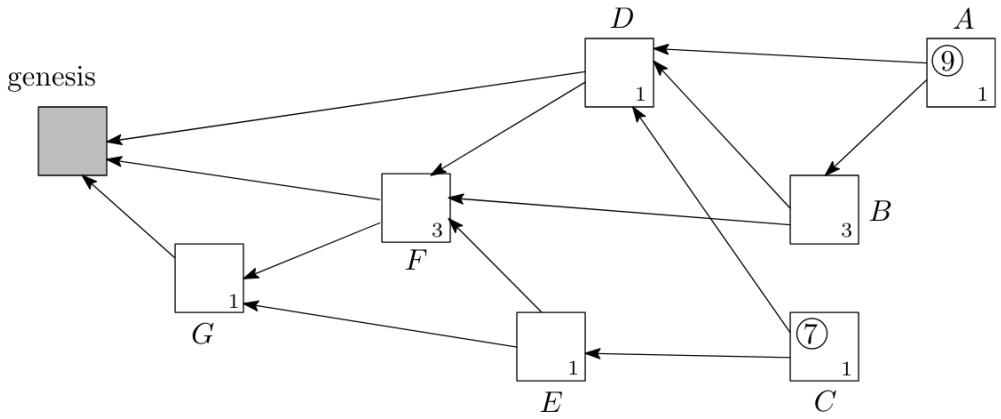

Figura 22 Cálculo de los puntajes de acuerdo a la altura y profundidad
Tomado de: https://iota.readme.io/docs/whitepaper Página 7

En la Figura 22, G tiene altura 1 y profundidad 3 (debido a la trayectoria inversa F, B, A), mientras que D tiene altura 2 y profundidad 2.

En el documento de IOTA whitepaper se describen con mayor detalle las secciones que explican la estabilidad del sistema tanto en situaciones con pequeño flujo de transacciones o de gran flujo de ella; además se explican las estrategias para la confirmación de transacciones y se modela el tiempo promedio de estimación en la aprobación de una transacción.

Con la finalidad de explicar la seguridad de este sistema, en la sección quinta del documento se enuncian los diferentes escenarios de ataque a los que puede ser sometida una Tangle, y como un factor diferenciador con respecto a la tecnología Blockchain la resistencia a ataques de computadores cuánticos.

En términos generales es una tecnología emergente que puede ser utilizada en las criptomonedas que favorece las pequeñas transacciones en un modelo representado por un grafo dirigido, que soporta mejor los ataques de computadores cuánticos que otros modelos como Blockchain.

3.4. Clasificación de tipos de DLT

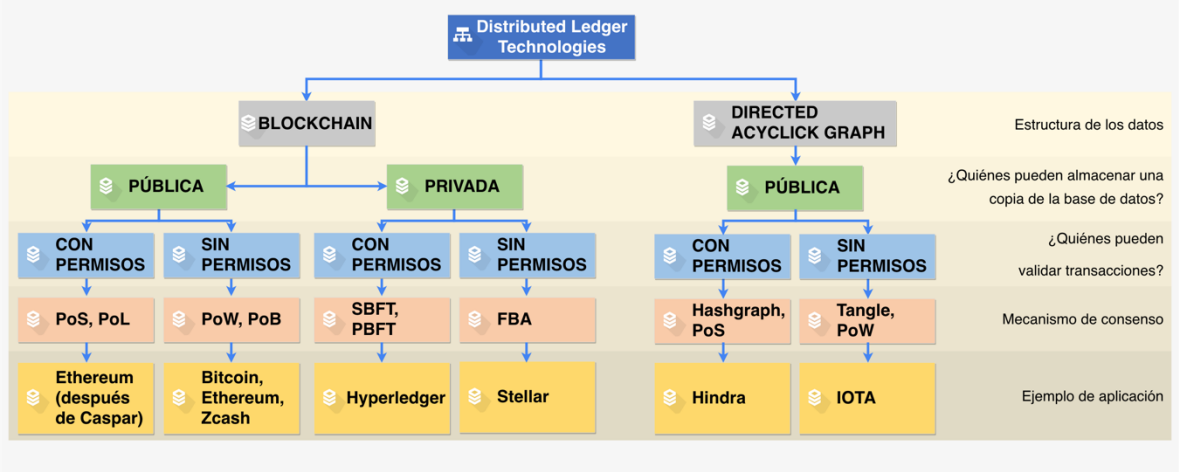

Figura 23 Clasificación de las DLT

Para clasificar los diferentes tipos de DLT se utilizan algunas características de estas, como lo son: i) la estructura de los datos, ii) la confidencialidad de las transacciones, iii) la validación de las transacciones y iv) el mecanismo de consenso. Finalmente se da un ejemplo de una aplicación que cumple con las 4 características previamente enunciadas.

Adicionalmente, y para clarificar lo incluido en la figura se incluye el siguiente glosario:

PoS	Proof of Stake
PoI	Proof of Identity
PoW	Proof of Work
PoB	Proof of Burn
SBFT	Simplified Bizantine Fault Tolerance
PBFT	Practical Bizantine Fault Tolerance
FBA	Federated Bizantine Agreement
Hashgraph	Nombre de la estructura de datos de Hedera
Tangle	Nombre de la estructura de datos de IOTA

Para clasificar los diferentes tipos de DLT se utilizan algunas características de estas, como lo son: i) la estructura de los datos, ii) la confidencialidad de las transacciones, iii) la validación

Ahora, a partir de la Figura, es importante realizar algunas precisiones, principalmente en lo relacionado con los Grafos Direccionados Acíclicos. Estos surgen principalmente con la motivación de mitigar algunos de los problemas de las DLT basadas en Blockchain y que tienen una característica pública, principalmente la capacidad para realizar transacciones de manera rápida.

Es por esto, que si bien en algunos casos se habla que las DLT basadas en DAG no tienen un mecanismo de consenso (debido a que este es implementado de manera automática en el

grafo), en el caso de Hedera y de IOTA como mecanismo de consenso se menciona la estructura del grafo (que es la misma estructura de los datos), pero estas dos soluciones adicionan un elemento de Proof of Stake y de Proof of Work respectivamente, motivo por el cual estas dos soluciones sí aparecen con un mecanismo de consenso en la figura. En el caso de Byteball, esta es una solución basada en DAG que no adiciona ningún mecanismo de consenso y por este motivo no se incluye alguno en la figura

4. ¿Qué se debe saber al implementar una DLT?

En este capítulo se brindarán las herramientas para implementar tecnologías DLT/Blockchain. Todos los esfuerzos implicados en el desarrollo e implementación tendrán mayor efectividad mediante la comprensión de los conceptos claves en un desarrollo de este tipo, tales como: arquitecturas, integración y tiempo, así como las ventajas y limitantes que esto conlleva.

A modo de introducción se considera importante que un desarrollador conozca las principales organizaciones públicas y privadas dedicadas a innovar y a desarrollar soluciones en DLT/Blockchain.

En la XXX se muestra el ecosistema de Innovación DLT/Blockchain a nivel mundial, dentro del que se destacan organizaciones como Bigchain DB, entidad referente a nivel mundial que cuenta con capacidades científicas, tecnológicas y comerciales, para desarrollar la tecnología DLT/Blockchain, que lo convierte en una empresa a resaltar en benchmarking para los emprendedores colombianos. Otras empresas que se pueden destacar son IBM, Sony y Siemens, que ya cuentan con patentes de aplicaciones basadas en DLT/Blockchain; también se resaltan los casos de organizaciones como BanQu Inc, BigchainDB GmbH, BitFlyer Inc, Blockchain Technologies Corp, Cambridge Blockchain LLC, Chronicled Inc, Cryptowerk Corp, Draglet GmbH Loyal, Corporation Medici Ventures INC, MonetaGo Inc, Othera PTY Ltd, Peer Ledger Inc y PeerNova Inc. (Superintendencia de Industria y Comercio, 2018).

Dentro del ecosistema de innovación DLT/Blockchain, también es importante resaltar el papel de universidades destacadas por su conocimiento científico para el desarrollo de la tecnología como Copenhagen y Surrey.

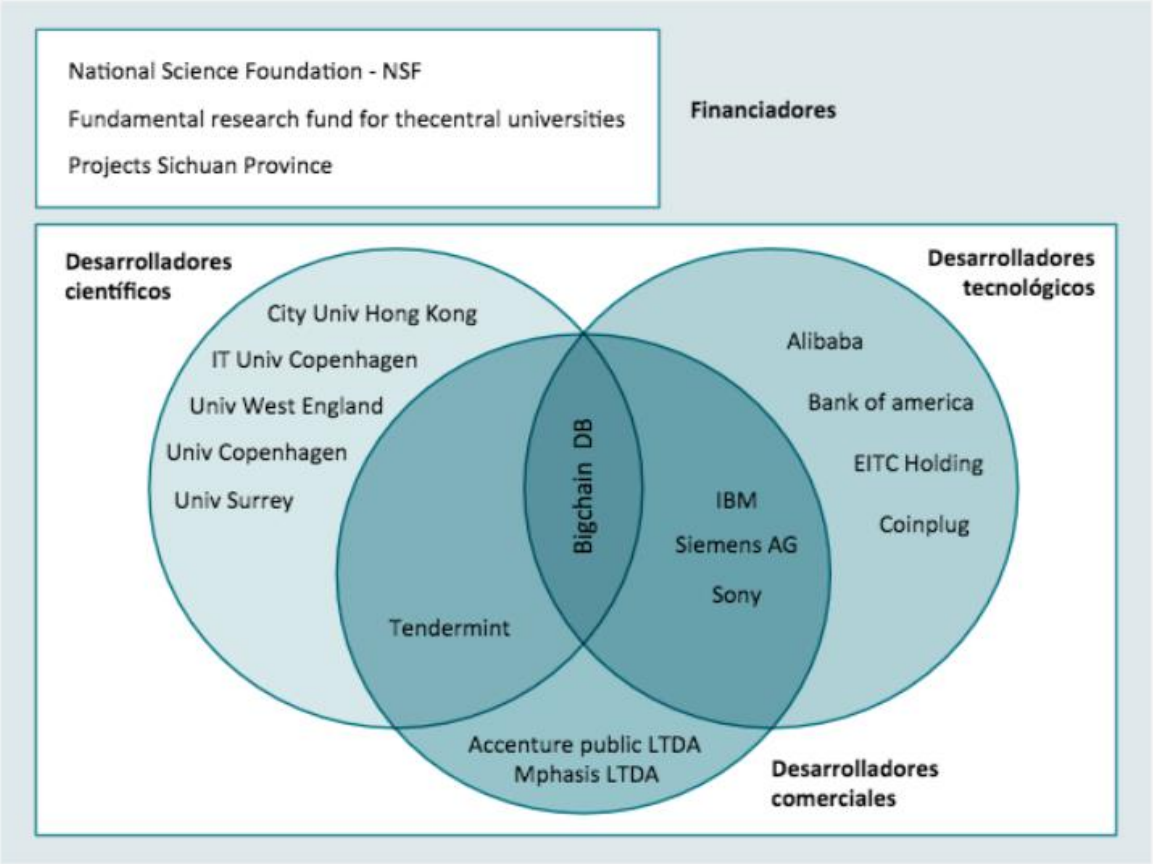

Figura 24 Ecosistema de innovación DLT/Blockchain a nivel mundial
Fuente: Bing, Scopus (2018)

4.1. Arquitectura Centralizada vs Arquitectura Descentralizada

La diferencia más notoria, y que hace que el surgimiento de DLT sea tan importante, es que en un sistema centralizado tradicional se encuentran múltiples entidades que generan transacciones, almacenándolas y validándolas con una sola unidad central, un solo servidor que procesa toda la información, y si el servidor es modificado, alterado, corrompido o atacado, las entidades conectadas a este se verán afectadas por los cambios de información.

En un sistema descentralizado DLT esto ya no es un problema, pues cada nodo tiene una copia en tiempo real de toda la información y cada nueva transacción es enviada, almacenada y validada por todos los nodos; de tal manera que si uno o varios nodos modifican, alteran, corrompen la información o sufren un ataque, las otras entidades sabrán

por un simple consenso de mayorías, que la información distribuida en alguno de ellos no es correcta; esto hace que los sistemas DLT sean más confiables que los tradicionales.

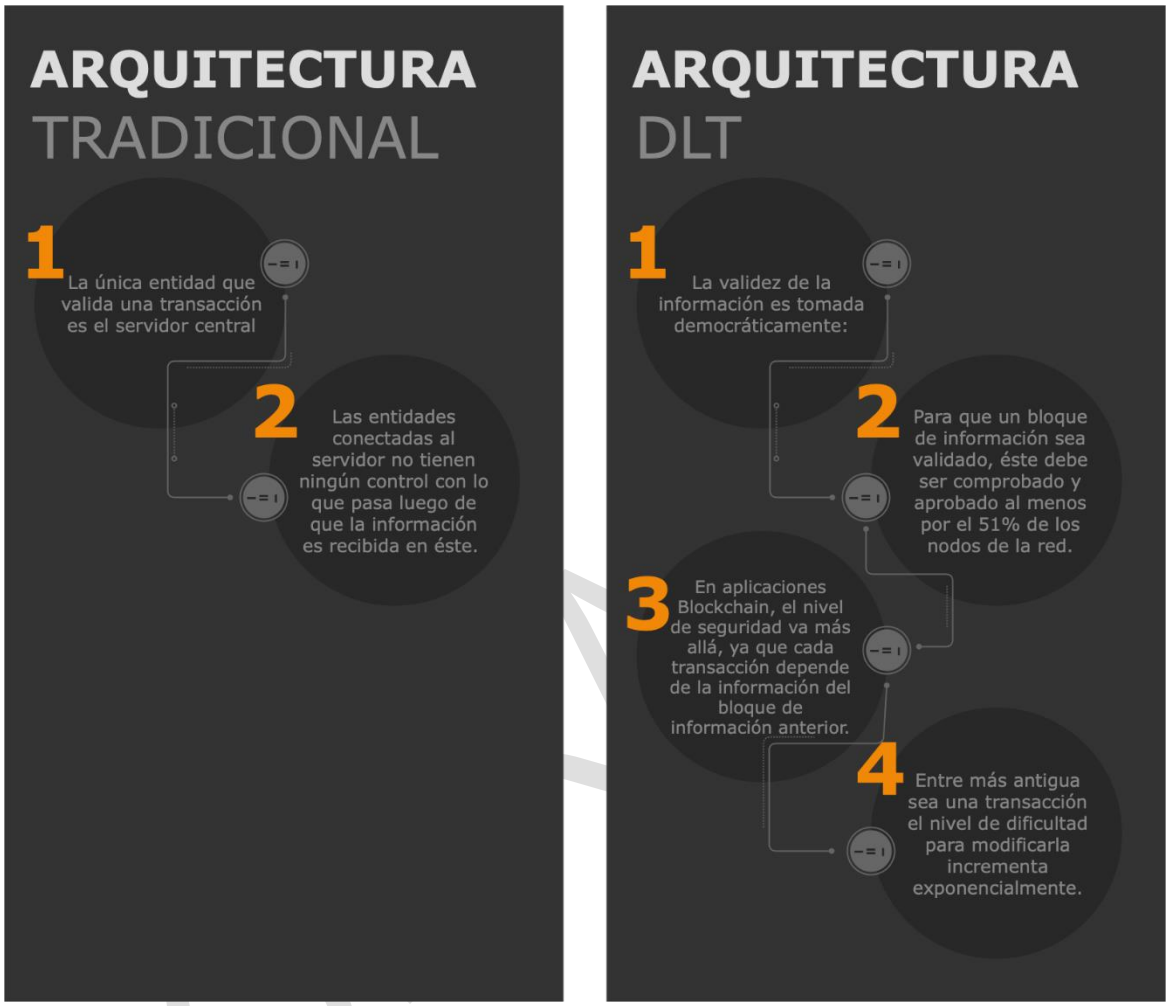

Figura 25 Comparación entre Arquitecturas Centralizadas y Descentralizadas

4.2. ¿Cómo hacer una integración DLT?

Blockchain es el tipo de implementación de DLT, sobre el cual se están centrando la mayoría de los esfuerzos en tecnologías libres o pagas que se pueden encontrar en el mercado.

Antes de empezar cualquier proyecto de software, los ingenieros hacen un listado y selección de tecnologías para el desarrollo de su sistema, tales como: Motor de base de datos, framework de desarrollo, librerías backend y frontend, entre otros, y de esta misma manera se puede hacer en un proyecto de software sobre un modelo DLT.

Tal como DLT, y en especial Blockchain, es una tecnología que se podría denominar como "tecnología emergente", también lo son los frameworks de desarrollo, comunidad y herramientas alrededor de ellas; por esta razón se debe ser cuidadoso y muy selectivo a la hora de la escogencia de alguna de éstas. Cada detalle y factor podrá ser determinante si se tienen en cuenta temas como mantenimiento y escalabilidad en un proyecto.

A continuación, se proponen 6 preguntas que se deben plantear un desarrollador antes de escoger una tecnología o un framework de desarrollo para DLT:

Figura 26 Metodología para identificar tecnologías o framework de desarrollo para DLT

4.3. Tipos de Frameworks

Algunos de los frameworks que se encuentran en el mercado son:

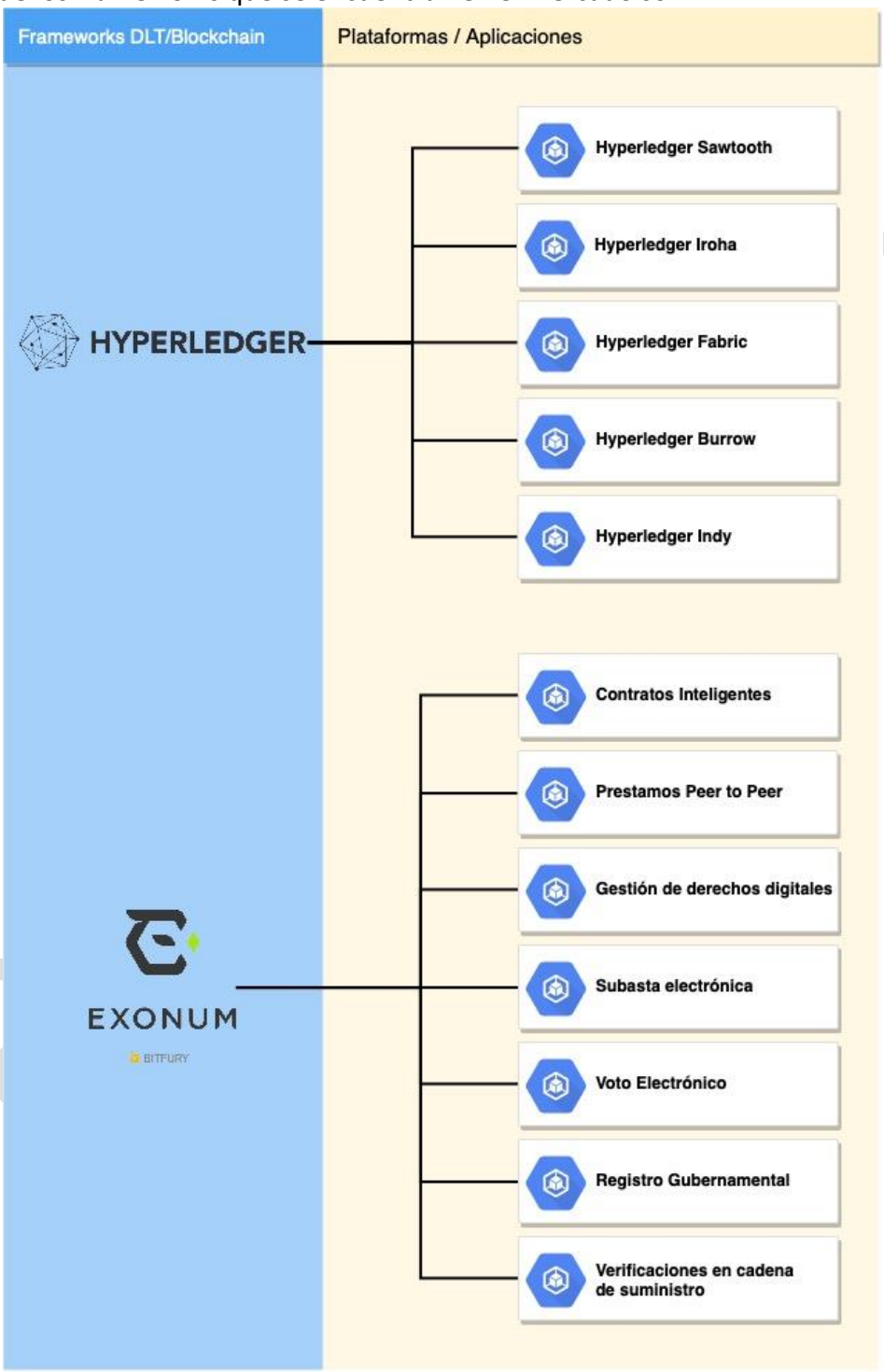

Figura 27 Tipos de Frameworks

Hyperledger:

Es un framework blockchain soportado por The Linux Foundation y tiene diferentes opciones dependiendo de la lógica del negocio que se quiera implementar, tiene opciones para soluciones móviles y ofrece frameworks con diferentes tipos de consenso (https://www.hyperledger.org/projects).

Exonum:

Es un framework para desarrollar aplicaciones descentralizadas sobre blockchain, utiliza el tipo de consenso Byzantine Fault Tolerant (https://exonum.com/es).

Tipos de aplicaciones con Exonum:

Contratos inteligentes.
Gestión de derechos digitales.
Voto electrónico
Verificaciones en cadenas de suministro.
Prestamos Peer to Peer.
Subasta electrónica.
Registro gubernamental.

Otras opciones (ver tabla 5)

Tabla 5 Otros tipos de Framework

HERRAMIENTA	LINK	DESCRIPCIÓN
Multichain	https://www.multichain.com/	Plataforma abierta para la construcción de blockchains. ● Desarrollo rápido ● Recursos ilimitados ● Data streams ● Cadenas privadas con permisos **Pros:** • Cuenta con una buena documentación. • Cuenta con buenos socios y aliados, entre ellos SAP. • A pesar de que está escrito en C++, cuenta con una interfaz JSON-RPC que puede ser usada con la mayoría de lenguajes modernos. **Contras:** • Es una licencia comercial, para su uso se debe pagar, su costo básico empieza en US$25.000
R3 Corda	https://github.com/corda/corda	Corda es un proyecto de blockchain de código abierto, diseñado para negocios desde el principio. ● Contratos inteligentes ● Funcionalidad de Notario ● Permite programación en JAVA **Pros:** • Es de código abierto. • Permite integraciones con JAVA. **Contras:** • Su comunidad aún no es muy grande.
Rootstock	https://www.rsk.co/	RSK (RootStock) es la primera plataforma de contratos inteligentes construido sobre el Blockchain de Bitcoin, su principal objetivo es agregar valor al ecosistema de Bitcoin. • Amigable con Bitcoin • Seguridad • Escalabilidad • Pagos instantáneos **Pros:** • Cuenta con cursos de entrenamiento, tanto a nivel de negocio como técnico. • Se soporta en una de las plataformas DLT Blockchain más robustas del mercado (Bitcoin). • Su desarrollo está sustentado en una comunidad creciente y un programa de afiliados. • Integraciones con JAVA

HERRAMIENTA	LINK	DESCRIPCIÓN
		Contras: • Es dependiente del Blockchain de Bitcoin.
Ethereum.org	https://www.ethereum.org/	Ethereum es una plataforma descentralizada que ejecuta contratos inteligentes: aplicaciones que se ejecutan exactamente según lo programado, sin ninguna posibilidad de inactividad, censura, fraude o interferencia de terceros. ● Dinero inteligente, billetera inteligente. ● Permite diseñar su propia criptomoneda. ● Permite crear una organización democrática. **Pros:** • Cuenta con una comunidad muy grande, tal vez la más grande en el universo del Blockchain y las criptomonedas. • Cuenta con un gran equipo, de expertos y profesionales que la soportan. • Ethereum registra alrededor de 700.000 transacciones al día. **Contras:** • Por la prueba de trabajo en la que está basado, sus transacciones son lentas y su red suele tener congestiones. • Los lenguajes de programación soportados no son muy populares, Solidity y Serpent.
BigchainDB	https://www.bigchaindb.com/	BigchainDB es una base de datos con características de blockchain, con alto rendimiento, baja latencia, potente funcionalidad de consulta, control descentralizado, almacenamiento de datos inmutables y soporte de activos integrado. **Pros:** • Permite queries NO SQL con MongoDB • Es altamente customizable. • Permite integraciones Públicas y Privadas. • Es de código abierto. • Permite integraciones con JAVA, PHYTON y JAVASCRIPT. **Contras:** • Su comunidad aún no es muy grande
Monax	https://monax.io/	Convierta los contratos en la columna vertebral de sus relaciones comerciales. Obtenga claridad, sepa dónde enfocar y cumplir los contratos de manera colaborativa. ● Crea tratos y acuerdos ● Lleva control de las obligaciones. ● Lleva control de la ejecución del contrato.

HERRAMIENTA	LINK	DESCRIPCIÓN
		Pros: • Es una plataforma en fase de producción para contratos inteligentes. • Documentación de integración por API lo cual permite su integración con la mayoría de lenguajes modernos. **Contras:** • El uso de Monax empieza desde $150 US al mes.

4.4. ¿Qué tanto tiempo y esfuerzo puede tomar hacer un proyecto con DLT y BLOCKCHAIN?

En teoría debería tardar lo mismo que un sistema tradicional, el problema reside en dos factores: el desconocimiento sobre la tecnología, encontrar personal capacitado no será tan sencillo y existirá la necesidad de capacitarlo; y las pruebas del sistema, que al ser un sistema descentralizado hace complicado emular pruebas automáticas y el proceso termina siendo muy manual.

El resto de los procesos en el desarrollo de un proyecto de software son los mismos, una vez se seleccionen las tecnologías, herramientas y frameworks a utilizar, la mayor parte del proceso de desarrollo se gastará en crear y validar la lógica del negocio.

El proceso de construcción y desarrollo podrá ser intrincado por la complejidad y el desconocimiento, pero al realizar una selección apropiada de la tecnología y un adecuado proceso de pruebas se podrá llegar a resultados viables y confiables, para ello se recomienda realizar pruebas pilotos rápidas, las cuales brinden resultados a bajo costo y en tiempos pequeños, considerando que dichas pruebas permiten validar la lógica del negocio y realizar replanteos en el proceso de la práctica.

4.5. Ventajas

Antes de listar las ventajas se muestran algunos hechos que, dado el momento en el que se encuentran las implementaciones DLT y en específico Blockchain, pueden ser aprovechados y tenidos en cuenta como ventajas.

- Los más entusiastas aseguran que no hubo una tecnología con un potencial disruptivo tan elevado desde la masificación de internet, hace ya 20 años. Tomado de: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/blockchain-una-idea-que-surge-a-partir-del-bitcoin-y-pretende-revolucionar-246240 (Campanario, 2018)

- La tecnología de criptomonedas y Blockchain está lejos de la “adopción masiva”, ya que solo 50 millones (0,71%) de los 7 mil millones de personas en todo el mundo los están utilizando, dijo un investigador de Blockchain: https://criptoinforme.com/menos-de-un-1-de-la-poblacion-mundial-usa-criptomonedas-la-adopcion-masiva-de-blockchain-tomara-tiempo-dice-un-investigador-de-criptografia/

- IBM ha invertido 200 millones de dólares en desarrollos asociados con blockchain: https://www.ccn.com/ibm-invests-200-million-in-iot-blockchain-development/ (Coleman, 2018)

- Los aplicativos y las tecnologías basadas en DLT/Blockchain podrían tener un valor económico de 8.000 millones de dólares: https://www.fin-tech.es/2017/01/informe-de-grand-view-research-sobre-blockchain-en-2024.html (Rodríguez, 2018)

- El 90% de los bancos del mundo están explorando el uso de DLT/blockchain: http://www.pulso.cl/tech/90-grandes-bancos-del-mundo-esperan-implementar-blockchain/ (Fajardo, 2018)

A continuación, se destacan las principales ventajas tecnológicas que han causado impacto desde el lanzamiento de la primera implementación de una solución comercial con Blockchain:

1. **Descentralización:** si se está interesado en soluciones DLT o Blockchain es seguramente porque se ha escuchado este término. Un sistema descentralizado tiene muchas ventajas cuando es combinado con otros términos como transparencia, autenticidad y seguridad; la descentralización permite que un sistema no tenga que depender de intermediarios o del control de algún ente o gobierno.

2. **Transparencia:** en la crisis financiera del 2008, que ocurrió en Estados Unidos con impactos en la economía mundial, uno de los mayores problemas fue la credibilidad en las instituciones financieras (Kotz, 2009) un sistema financiero sobre DLT Blockchain permite a sus miembros tener el control de los recursos y transacciones, evitando fraudes o modificaciones en la información gracias a los tipo de consenso previamente explicados.

3. **Inmutabilidad:** cuando la información es controlada por una sola entidad, los "hackers" solo tienen que entrar en ésta y corromper la información, con DLT Blockchain los atacantes tendrían que corromper la información del 51% de las personas o entidades interactuando con la información (Nodos) y todo esto al mismo tiempo.

4. **Seguridad:** la mayoría de los tipos de DLT y Blockchain se sustentan en algoritmos criptográficos complejos que hacen que sea difícil realizar cambios en la información o corromper el consenso descentralizado.

5. **Autenticidad:** algo importante a aclarar es que existen implementaciones DLT tanto públicas como privadas, y aun así sea de forma anónima o no, todas las transacciones garantizan la autenticidad de los datos, es decir quien o quienes son los dueños de la transacción o información.

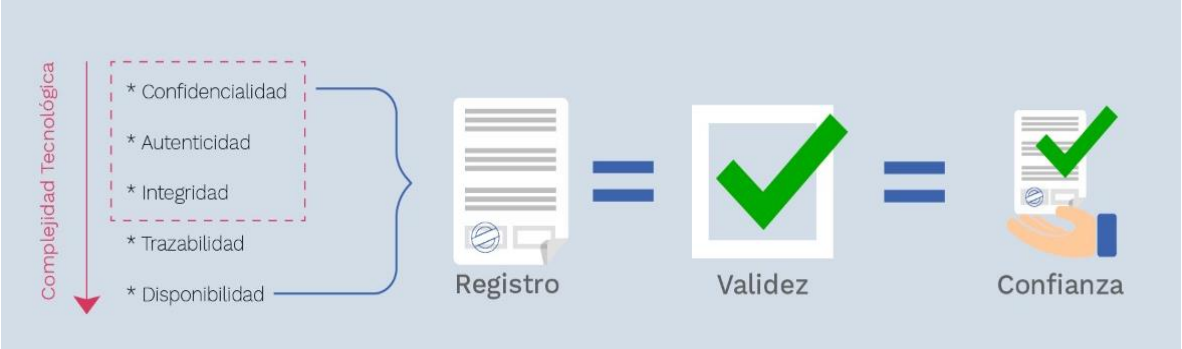

Figura 28 DLT como generadora de confianza a través de registros válidos

La tecnología DLT se considera una innovación en la forma en que se pueden digitalizar una transacción, debido a que por medio de ella se logra garantizar las siguientes características:

1. Otorgamiento de confianza a un archivo digital en un mayor o igual grado que un documento físico.

2. La validez de un documento es otorgada a través de un proceso democrático, no de forma centralizada.

Para lograr **CONFIANZA** en los usuarios la tecnología DLT se basa en el fortalecimiento y gestión de la integridad, autenticidad, confidencialidad, disponibilidad y trazabilidad.

4.6. Limitantes

Las limitantes de esta tecnología son una mezcla entre aspectos técnico/tecnológicos y sociopolíticos. Otro aspecto importante a resaltar, es que la mayoría de los retos y problemas que se han encontrado en el uso de aplicaciones sobre DLT y Blockchain han sido sobre un puñado pequeño de sistemas que se encuentran en producción, en especial en criptomonedas como Bitcoin y Etherium, con mucha más relevancia el primero. Las mayores limitantes de esta tecnología son:

1. **Conocimiento y estado del arte:** en la actualidad el nivel de productividad académica y comercial de la tecnología DLT en Colombia es incipiente; basta con hacer una revisión bibliográfica en bases de datos como Scopus, para identificar tan solo 12 artículos asociados con la tecnología DLT/Blockchain en nuestro país, donde las más antiguas datan del año 2016 y 9 de ellos abordan el tema de los criptoactivos. La Tabla 6 , muestra los artículos identificados en Scopus relacionados con la tecnología DLT en otras áreas diferentes a las de los criptoactivos.

Tabla 6 Artículos identificados en la base de Scopus

NOMBRE	ÁREA	AÑO	DESCRIPCIÓN
Document management system based on a private Blockchain for the support of the judicial embargoes process in Colombia.	Judicial	2018	Aplicación piloto que permite la publicación y distribución de documentos de embargo, dentro de un sistema de gestión de documentos que, garantiza la confidencialidad, disponibilidad y fiabilidad de toda la información registrada en el Blockchain.
Methodological approach to the definition of a Blockchain system for the food industry supply chain traceability	Alimentos	2018	Metodología para integrar la tecnología Blockchain en la cadena de suministro de la industria alimentaria, que permite la trazabilidad a lo largo del proceso y proporciona al cliente final la información suficiente sobre el origen del producto para tomar una decisión de compra informada.
Diseño de la Arquitectura de un Sistema de Contratos Inteligentes Basada en la Tecnología Blockchain Aplicada al Proceso de Registro de Estudiantes en el Sistema de Educación Colombiano	Educación	2018	Desarrollo de una arquitectura para un sistema de información, basado en contratos inteligentes por medio de tecnología Blockchain para el registro de estudiantes en el sistema educativo.

Búsquedas académicas en la base de datos de Google Scholar asociadas a la tecnología DLT/Blockchain también muestran trabajos de grupos de investigación colombianos en áreas diferentes a los criptoactivos desde el año 2016. Los artículos que se relacionan en la Tabla 7:

Tabla 7 Artículos identificados en Google Scholar

NOMBRE	ÁREA	AÑO	DESCRIPCIÓN
BC-MED: Plataforma de Registros Médicos Electrónicos Sobre Tecnología Blockchain	Salud	2018	Diseño de la plataforma BD-MED por medio de Blockchain para el acceso, registro y almacenamiento del historial clínico de los pacientes, incluso en escenarios con fallas de conectividad.
Tratamiento Jurídico de las Transacciones Comerciales con BITCOINS en Colombia	Jurídica	2017	Se expone información sobre el comercio por medio de las nuevas tecnologías ya que ha sido un motor de crecimiento y desarrollo del comercio electrónico.

NOMBRE	ÁREA	AÑO	DESCRIPCIÓN
Mercado eléctrico en Colombia: transición hacia una arquitectura descentralizada	Tecnológica	2018	Este trabajo presenta las características de la electricidad como bien económico y compara la evolución del mercado eléctrico del Reino Unido (la experiencia original) con el de Colombia, discute los problemas centrales del modelo colombiano e identifica oportunidades para la implementación de una arquitectura descentralizada en Colombia.
Desarrollo de un Prototipo Basado en Blockchain Aplicado a la Plataforma IoT Sobre un Sistema Embebido	Ciudades Inteligentes	2018	Describe la implementación paso a paso de un contrato inteligente con un dispositivo IoT para la generación de alertas en la medición de una variable de contaminación del medio ambiente, con el fin de tener más seguridad y control a través de dispositivos conectados a internet a la hora de medir estos niveles de contaminación en una ciudad inteligente.

2. **Escalabilidad:** este es tal vez el mayor problema al que se enfrenta esta tecnología, relacionado a aspectos técnicos como latencia de transacciones y limitantes de espacio y procesamiento. Como las soluciones DLT proponen que cada nodo del sistema tenga una copia de toda la información hace que por ejemplo para generar un nodo adicional de Bitcoin, hoy se requiere mínimo 500GB de espacio en disco y 5GB adicionales mensuales.

   Y por el lado de la latencia, para ponerlo en contexto, imaginen tener que esperar entre 15 y 30 minutos en la red bitcoin para una transacción. Hoy los desarrolladores están trabajando en soluciones híbridas donde un conjunto de transacciones y datos son tratados fuera del Blockchain (sistemas tradicionales), para luego en casos específicos validarlos dentro del Blockchain.

3. **Falta de regulaciones:** esta es tanto una ventaja como una desventaja. Aplicaciones como Bitcoin definitivamente han sacado el mejor provecho de ésta, pero en realidad es una limitante tanto para soluciones DLT como tradicionales, un caso puntual es Uber como aplicación tecnológicamente tradicional.

5. Casos de estudio sobre DLT

En este capítulo se presentan en principio una visión general de las posibles aplicaciones de DLT/Blockchain y posteriormente se hace énfasis en casos de estudio específicos asociados

a diversos sectores como gobierno (gestión de identidad, salud, educación, sistema de votación, contratos inteligentes y registros de autenticidad de tierras), industria del entretenimiento y logística.

En la Figura 29 se presentan los principales usos registrados de la tecnología hasta el momento.

Por su parte CompTIA en el documento *"Harnessing the Blockchain Revolution: CompTIA's Practical Guide for the Public Sector"*, menciona algunos de los productos que existen o que podríamos esperar ver en un futuro cercando siendo implementados y ofrecidos para el sector público, los cuales se muestran en la Figura 29.

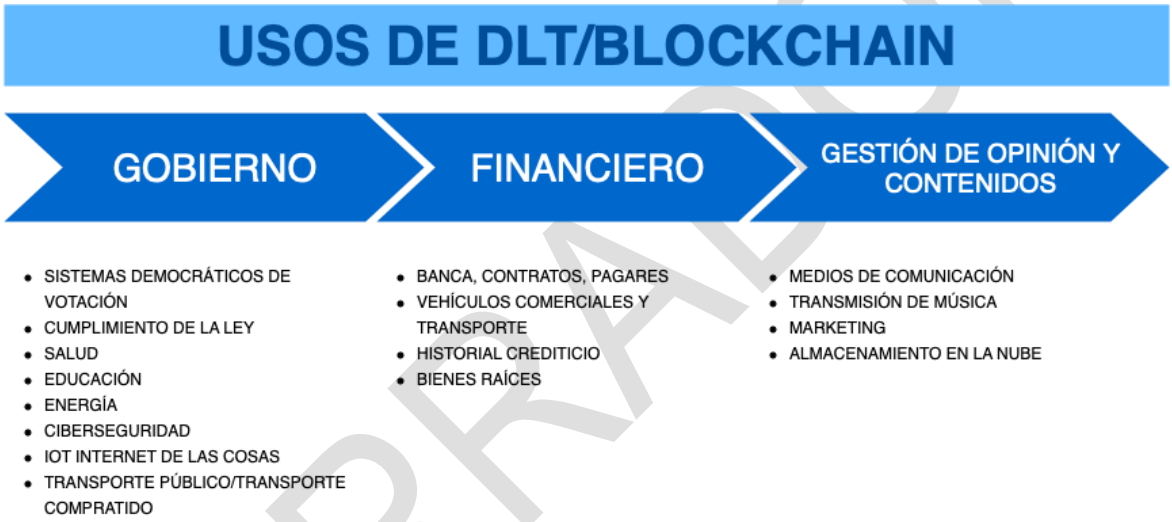

Figura 29 Productos y servicios basados en DLT/Blockchain para el sector público

En la Figura 30, se muestran la relación de número de productos e invenciones de I+D relacionadas con DLT/Blockchain, en donde se hace evidente el liderazgo de China y Estados unidos, al tiempo que se muestra una producción incipiente en Latinoamérica.

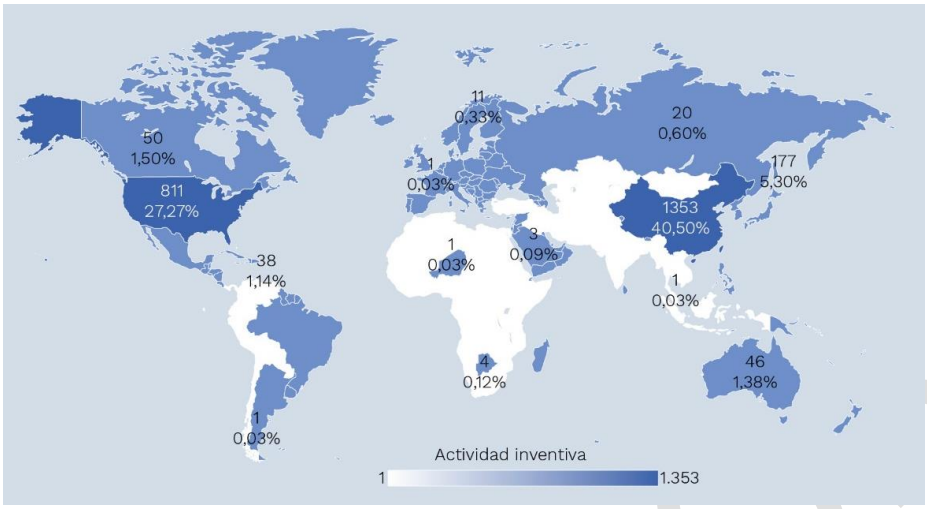

Figura 30 Países líderes en solicitudes de patentes
Fuente Derwent Innovation, Espacenet, USPTO, Latipat, entre otras (2018)

De igual forma en la Figura 31, se pueden encontrar redes de colaboración entre los solicitantes de patentes basadas en el desarrollo de la tecnología DLT/Blockchain. La mayor red de colaboración de solicitantes está conformada por 22 solicitantes. Se pueden destacar los trabajos desarrollados por Samsung e IBM, que tienen una participación activa en las redes de colaboración y la inversión que están haciendo para mejorar el desarrollo de la tecnología.

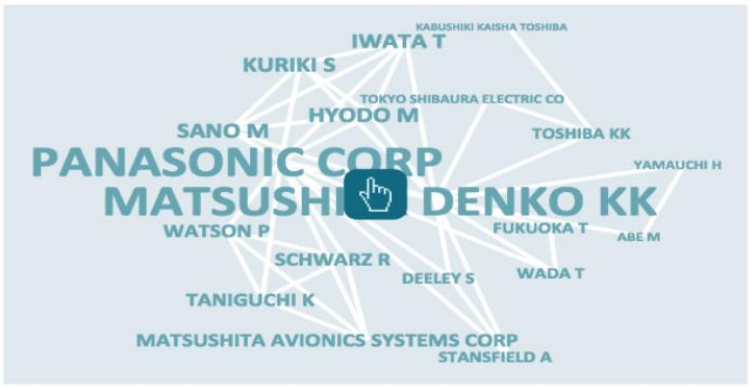

Figura 31 Redes de colaboración entre solicitantes
Fuente: Derwent Innovation, Espacenet, USPTO, Latipat, entre otras (2018)

5.1. Gobierno

El sector gobierno puede verse beneficiado con el uso de DLT/Blockchain porque con su uso se pueden obtener múltiples ventajas como ahorros de tiempo en trámites, uso de cero papeles, trazabilidad en la gestión contractual, seguimiento de la entrega de los subsidios,

lucha contra el contrabando y reducción de distribución de productos falsificados. A continuación, se describe casos específicos de uso en el sector gobierno:

Sistemas de votación

La tecnología DLT/Blockchain se puede utilizar para realizar procesos de votación transparentes. Con un sistema de votación sobre DLT/Blockchain se puede eliminar muchos intermediarios; actualmente se selecciona a personas naturales para que ejerzan como jurados, sin verificar un perfil y sin comprobar una capacidad específica para ejercer el cargo, y son seleccionados aleatoriamente miles de jurados. Usando DLT/Blockchain cada ciudadano puede enviar su voto anónimo a la cadena de bloques, además, los resultados de las votaciones al quedar registrados no se pueden modificar. Esto elimina la sobrecarga considerable del entorno de votación, desde la preparación hasta la tecnología, el personal y los recuentos (Kakavand, Kost De Sevres, & Chilton, 2017). Esta tendencia no es ajena a Colombia, donde la Alcaldía de Bogotá en colaboración con investigadores del ViveLab de la Universidad Nacional desarrolló una solución para realizar las elecciones de personeros en algunos colegios de la ciudad (Alcaldía de Bogotá, 2018).

Contratos Inteligentes

Una de las aplicaciones de la tecnología DLT/Blockchain, que ha aumentado en su auge en los últimos años son los contratos inteligentes; los términos que conforman un contrato inteligente se codifican y se cargan en los registros, generando un contrato descentralizado donde no se necesita de un tercero para el registro o la ejecución del mismo.

Datos importantes para tener en cuenta en contratos inteligentes:

- Las cláusulas contractuales implícitas en el contrato se ejecutan de manera automática, cuando se cumplen las condiciones estipuladas, eliminando la ambigüedad que se pueda presentar en los términos estipulados en los acuerdos y los conflictos respecto a dependencias externas.

- Los contratos inteligentes son protocolos informáticos que facilitan, verifican o imponen la negociación o ejecución de un contrato, o que hacen que una cláusula contractual sea innecesaria; generalmente también tienen una interfaz de usuario y, a menudo, emulan la lógica de las cláusulas contractuales. Bajo el diseño de contratos inteligentes, muchos tipos de cláusulas contractuales pueden, por lo tanto, hacerse parcial o totalmente auto-ejecutables. Los contratos inteligentes tienen como objetivo proporcionar seguridad superior al derecho contractual tradicional y reducir otros costos de transacción asociados con la contratación.

Nota: una característica fundamental de Blockchain para la implementación de contratos inteligentes es la posibilidad de efectuar transacciones "con confianza"; es decir, transacciones que pueden validarse, monitorearse y ejecutarse bilateralmente a través de una red digital sin la necesidad de un intermediario externo de confianza. La funcionalidad de firma múltiple se puede incorporar en contratos inteligentes donde se requiere la aprobación de dos o más partes antes de que se pueda ejecutar algún aspecto del contrato. Cuando las condiciones de un contrato inteligente dependen de datos del mundo real, se pueden desarrollar sistemas externos acordados llamados "oráculos" para monitorear y verificar precios, desempeño u otros eventos del mundo real.

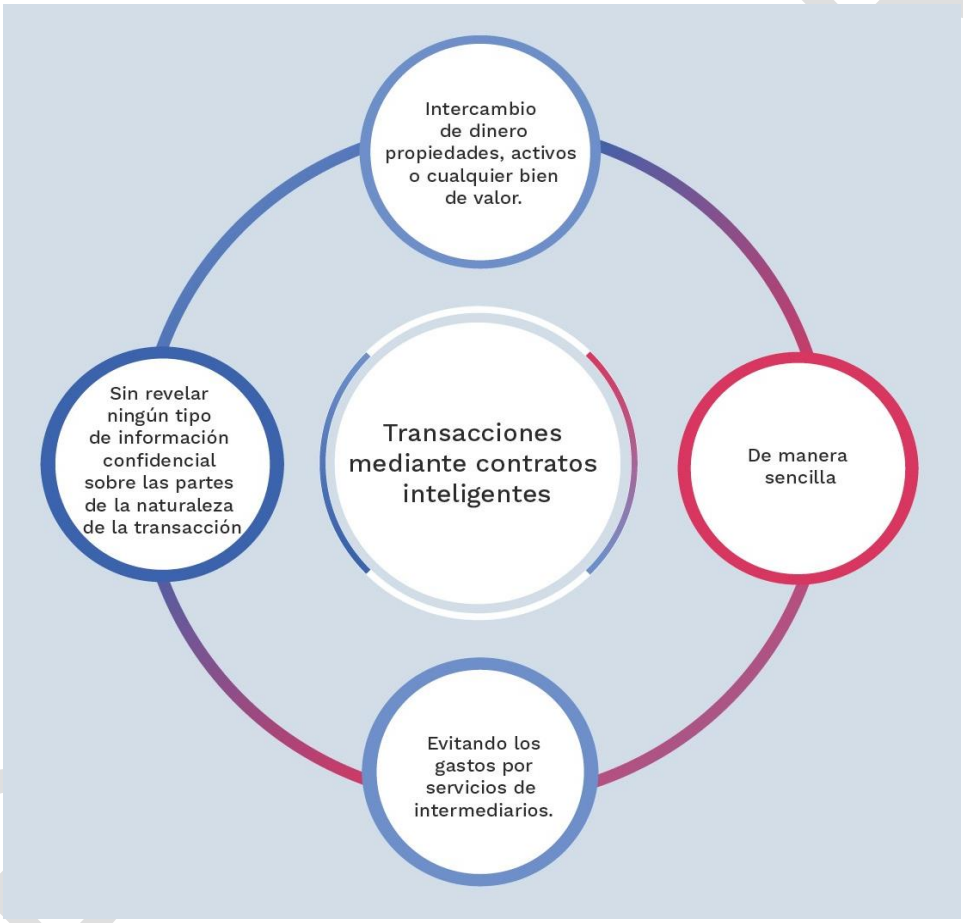

Figura 32 Transacciones mediante contratos inteligentes

¿Qué son las transacciones financieras para los contratos inteligentes?

Los contratos inteligentes se pueden codificar de manera tal que el pago, la compensación y la liquidación se realicen automáticamente de manera descentralizada sin la necesidad de un intermediario externo (Houman, 2014). Por ejemplo, un contrato de derivados inteligentes podría reprogramarse con todos los términos contractuales (es decir, calidad, cantidad, entrega), excepto el precio, que podría determinarse algorítmicamente a partir

de los datos del mercado suministrados a través de un oráculo. El margen podría transferirse automáticamente en llamadas de margen y el contrato podría rescindirse en caso de incumplimiento de la contraparte.

¿Qué permiten los contratos inteligentes?

El intercambio de dinero, propiedades, activos o cualquier bien de valor de una manera sencilla, evitando los gastos por el servicio de intermediarios y sin revelar ningún tipo de información confidencial sobre las partes la naturaleza de la transacción. Para ilustrar mejor el desarrollo de un contrato inteligente, consideremos la venta o el alquiler de un vehículo, implementando la tecnología DLT/Blockchain a través del pago con monedas digitales; la persona que desea adquirir el vehículo obtiene un recibo, que en este caso se considera un contrato inteligente y la llave digital que llega a este en la fecha especificada; en caso de que la llave no llega a tiempo, se le reembolsa el dinero al cliente, si llega, ambas partes reciben lo acordado a tiempo.

La Autoridad Europea de Valores y Mercados (ESMA) afirma sobre DLT/blockchain: *"los contratos inteligentes, que se ubican encima de los libros de contabilidad, pueden ayudar a reducir la incertidumbre asociada a los términos del contrato y aumentar la automatización del procesamiento de acciones corporativas, incluso si su uso puede ser limitado a ciertos tipos de instrumentos o contratos por razones de complejidad, al menos en el corto plazo. [...]. Los contratos inteligentes son códigos de ejecución automática destinados a replicar los términos de un contrato determinado. Ellos traducen efectivamente los términos contractuales (por ejemplo, términos y condiciones de pago, acuerdos de confidencialidad) a material computacional".* (Kakavand, Kost De Sevres, & Chilton, 2017).

Educación

Actualmente los títulos académicos formales (pregrados, especializaciones, maestrías y doctorados) no permiten determinar la capacidad y conocimiento de las personas al presentar su curriculum vitae; el aprendizaje no formal adquirido también es necesario y apreciado en las diferentes empresas en los procesos de contratación, los cuales se validan por medio de mecanismos internos en los procesos de selección (Bartolomé, Bellver, Castañeda, & Adell, 2017).

Al momento de las compañías solicitar un currículo vitae a una persona en un proceso de selección, este es elaborado por el propio aspirante, donde dicho documento no acredita la veracidad de los títulos y conocimientos que expone el aspirante; por otro lado, el proceso de recolección de los certificados que garantizan los títulos obtenidos por el aspirante y la comprobación por parte de la empresa se convierte en un proceso complejo.

Figura 33 Problemas derivados de premisas anteriores en sector educación

Para dar solución a la veracidad de la información presentada por un aspirante en un proceso de selección, se debería establecer una entidad central que garantice la información expuesta. En la actualidad se pueden encontrar identificadores institucionales que garantizan la información como el sistema GREC de la universidad de Barcelona, este permite verificar de forma correcta los títulos, pero deja abierta la posibilidad para que se verifiquen las competencias adquiridas por los aspirantes y los conocimientos desarrollados en programas de educación no formal (Bartolomé, Bellver, Castañeda, & Adell, 2017).

En materia del ámbito de investigación:
Se pueden encontrar sistemas que garantizan la producción científica de un investigador como Google Scholar, OrcID, el Researcher ID, o redes como Research Gate, Academia.edu o Mendeley, para citar algunos, los cuales han permitido automatizar la recolección de dicha información científica.

La adecuada implementación de Blockchain permitiría acreditar la información suministrada por los aspirantes en un curriculum vitae, de tal forma que se pueda contrarrestar la manipulación de la información suministrada, convirtiendo este sistema en una especie de "*moneda intelectual*". Un uso educativo obvio es almacenar registros de logros y créditos, como certificados de grado. Los datos del certificado serían agregados al Blockchain por la institución que los otorga, a la que el estudiante puede acceder, compartir con los empleadores o generar un enlace desde un curriculum vitae en línea. Se abren oportunidades para la concesión directa de certificados y distintivos por parte de expertos y maestros de confianza (Sharples & Domingue, 2016). Algunas experiencias en la implementación vienen dadas por:

- La Universidad de Nicosia (Chipre) es la primera institución de educación superior en emitir certificados académicos cuya autenticidad puede verificarse a través de Blockchain (University of Nicosia, 2017); las características de la plataforma y el diseño del Blockchain se pueden encontrar en la página web: https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/.

- Sony Global - Sony Global - Sony Global Education ha desarrollado una tecnología que aplica blockchain al campo educativo, aprovechando las propiedades seguras de blockchain para realizar la transmisión cifrada de datos, como los registros de competencia académica de un individuo y las medidas de progreso, entre dos partes específicas. La tecnología tiene el potencial de realizar un sistema de infraestructura completamente nuevo para compartir registros de forma segura a través de la red en cualquier número de formas, abriendo nuevas puertas de posibilidades para los registros académicos y cómo se evalúan (Sony Global Education, 2016)

Posiblemente el primer intento de trabajar en esta solución lo haya puesto en marcha el MIT Media Lab en 2015, cuando comenzó a distribuir certificados a los participantes en su programa de becas adjuntas a la dirección (Director's Fellows program) autentificados mediante la tecnología DLT/Blockchain (Raths, 2016). Devine (2015) lo define como una posible transferencia universal de créditos entre instituciones.

Salud

Existen múltiples aplicaciones de la tecnología DLT/Blockchain para la industria de la salud, incluida la distribución de productos y servicios. Un caso específico es el suministro de medicamentos desde la planta hasta el usuario final, por lo que los paquetes de medicamentos se autentican y se sellan en el tiempo en cada punto de entrega intermedio.

Por ejemplo: para un lote de medicamentos que se envían desde el piso de la fábrica, el registro de lote se autentica, se marca con la hora, se coloca en DLT/Blockchain, se autentica y se marca de nuevo en cada punto de entrega intermedio.

¿Beneficios en el sector salud?

El seguimiento del medicamento a medida que se abre paso a través del proceso de entrega. Esto simplifica y agiliza en gran medida la gestión de la distribución de medicamentos que puede evitar que caigan en las manos equivocadas, autenticando el medicamento para el consumidor final, lo que reduce en gran medida la posibilidad de falsificación, la manipulación de precios y la entrega de medicamentos vencidos.

A continuación se presenta en la Tabla 8 las oportunidades, desafíos e interesados de estudios realizados por el Reino Unido para la implementación de DLT/Blockchain en el sector de la salud (Deshpande, Stewart, & Lepeti, 2017):

Tabla 8 Implementación de la Tecnología DLT/Blockchain en el sector salud

OPORTUNIDADES	DESAFÍOS	INTERESADOS

Nuevos flujos de ingresos y modelos de negocio basados en registros de datos de salud del paciente. Reducir los costos de transacción a través de la desintermediación. Permitir que los pacientes conserven el control sobre los datos individuales.	Dependencia de un solo proveedor. No ha sido probado en grandes plataformas de infraestructura de salud. Mayor riesgo de seguridad en ausencia de casos de uso del mundo real viables.	Los departamentos gubernamentales de salud. Proveedores de salud independientes / privados. Pacientes / organizaciones que representan los intereses y derechos de los pacientes. Cuidadores profesionales o familiares de pacientes. Aseguradoras de salud.

De igual forma, las empresas del sector farmacéutico presentan un conjunto de desafíos, oportunidades e interesados, los cuales se presentan en la Tabla 9.

Tabla 9 Implementación de la tecnología DLT/Blockchain en la industria farmacéutica

OPORTUNIDADES	DESAFÍOS	INTERESADOS
Importancia para la protección de la propiedad intelectual y el registro de datos de las cadenas de suministro. Mejorar la eficiencia de la distribución de medicamentos. Reducir la falsificación.	Mayor riesgo de seguridad en ausencia de casos de uso del mundo real viables. Posibles conflictos o diferencias con los enfoques existentes para ensayos clínicos, pruebas de medicamentos y cumplimiento normativo. Uso limitado a la prueba de concepto para cadenas de suministro farmacéuticas.	Las empresas farmacéuticas. Reguladores del sector farmacéutico. Organizaciones involucradas en la distribución farmacéutica. Usuarios finales / organizaciones que representan los intereses y derechos de los usuarios finales. Profesionales de la salud. Los fabricantes forman parte de la cadena de suministro farmacéutica. Los minoristas farmacéuticos.

Sistemas de registro de propiedad

Las aplicaciones de la tecnología DLT/Blockchain en la industria de bienes raíces pueden aplicarse tanto al sector público como al privado. En el sector público, el registro de la propiedad y los registros públicos de la propiedad de la tierra se pueden colocar en una plataforma bajo tecnología DLT/Blockchain, lo que permite a las partes interesadas y agencias relevantes acceder en tiempo real a los registros de la propiedad; esto reduce considerablemente las disputas de propiedad y la necesidad de intermediarios para autenticar documentos y adjudicar disputas, lo que en última instancia ahorra costos y tiempo para el consumidor final.

Ejemplo: en la actualidad el gobierno de Honduras, ha contratado una empresa de Estados Unidos para construir un sistema de registro de títulos de propiedad permanente y seguro utilizando tecnología DLT/Blockchain (Reuters News - http://in.reuters.com/article/usa-honduras-technology-idINKBN0O01V720150515). Dentro del sector privado, los contratos de alquiler residencial entre contrapartes privadas pueden colocarse en Blockchain y ejecutarse mediante contratos inteligentes. Esto agilizará los contratos privados y el flujo de trabajo de las agencias inmobiliarias, ahorrando recursos y tiempo.

Dentro del sector privado, los contratos de alquiler residencial entre contrapartes privadas pueden colocarse en Blockchain y ejecutarse mediante contratos inteligentes.

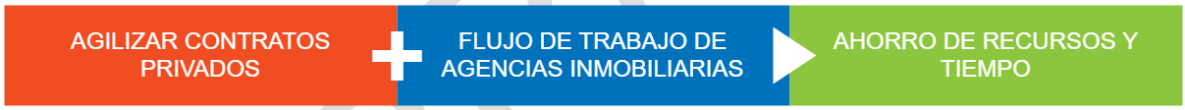

Figura 34 Resultado de implementar tecnología DLT/Blockchain en la industria inmobiliaria

Los contratos de alquiler residencial entre contrapartes privadas pueden colocarse en una plataforma DLT/Blockchain y ejecutarse mediante contratos inteligentes como ya mencionamos anteriormente; esto agilizará los contratos públicos y privados, y el flujo de trabajo de las agencias inmobiliarias, ahorrando recursos y tiempo. Se pueden eliminar intermediarios como notarías, agencias inmobiliarias y optimizar los procesos de repartición de tierras en Colombia como la Agencia Nacional de Tierras. Los activos de información en este proceso son los títulos de tierras, contratos, que tienen valor, se pueden transferir y se pueden ejecutar. Se puede considerar como ejemplo de aplicación en Colombia, el proyecto entre ViveLab Bogotá y el grupo de investigación InTIColombia de la Universidad Nacional, que busca asegurar la información de parte de los procesos de restitución de tierras por medio de DLT. El proceso de restitución de un predio tiene varias etapas; en esta cadena de procedimientos, el proyecto se plantea, justo después de que un juez expide la resolución que restituye una tierra a un individuo, ahí entra la plataforma DLT, en la que se consignan los datos del predio y del propietario.

Gestión de Identidad

La gestión de identidad es muy importante en el proceso de verificación sobre el poseedor de documentos de identificación como el pasaporte o la cedula de ciudadanía, y en general sobre todo registros públicos que se asocie a un ciudadano. Las soluciones para la gestión de identidades en DLT/Blockchain son aún emergentes, sin embargo, se están realizando una cantidad considerable de trabajos sobre este tema, en especial sobre pasaportes y licencias de conducción.

El gobierno de Estonia está experimentando con soluciones de gestión de identidad en DLT/Blockchain; lo utilizará para los actos legales incluido el matrimonio; aunque el primer matrimonio certificado utilizando tecnología DLT/Blockchain se dio en Williamsburg, Brooklyn (Woods, 2015).

5.2. Seguimiento de cadenas de suministro

La Cámara de Comercio Internacional estima que el valor total de productos falsificados y pirateados ascendió a US $ 1.77 billones en el año 2015. Con más productos falsificados en el mercado, los consumidores tienen una necesidad aún mayor de encontrar proveedores confiables e información de calidad, ya que existen muchos peligros en el uso de productos falsificados.

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) advierte a los consumidores que la compra de productos falsificados puede costarles más que solo pérdidas financieras; el uso de productos falsificados puede causar enfermedades, discapacidades o incluso la muerte. La comida es un área donde la confianza es primordial; la fórmula de leche contaminada que contiene melamina, un producto químico que se usa normalmente en los plásticos enfermó a 300.000 bebés chinos en 2008, de los cuales aproximadamente 54.000 fueron hospitalizados y seis murieron. También se han reportado casos en los que se ha encontrado veneno para ratas y otros químicos peligrosos en los alimentos reemplazando otros aditivos más caros y legítimos que deberían haber sido usados.

Muchas marcas importantes han hecho grandes esfuerzos en generar confianza al hacer que el proceso de creación y envío de sus productos sea más transparente. Se ha intentado probar el valor, la frescura y la autenticidad de los productos cotidianos que utilizan algún software de seguimiento hasta hoy, pero la entrega de esos datos o la confiabilidad de ese sistema de entrega simplemente no ha sido lo suficientemente buena. Los consumidores todavía tienen que confiar en cualquiera de los datos ingresados en el sistema, y podrían haber sido editados después del hecho también.

Existen al menos una docena de sistemas de seguimiento de software heredados que pueden seguir un artículo del productor a la tienda, y contarnos algo al respecto en línea, pero desde el punto de vista del consumidor, ¿por qué debemos confiar en sus datos? Los productores crean y controlan toda esa información, no los consumidores, ni siquiera el gobierno, por lo que si hay alguna duda sobre dónde se originó la bolsa de Gucci o qué edad tiene el salmón, sería ingenuo no preguntar por qué no podrían simplemente informar erróneamente o falsifique completamente los números cuando sea en su beneficio hacerlo.

Provenance es la primera empresa en intensificar y crear estas cadenas de suministro transparentes para todo tipo de productos basados en tecnología Blockchain. Si bien algunos servicios especializados como Everledger y Ascribe utilizan la Blockchain para rastrear tipos de productos individuales, en sus casos de diamantes y arte digital, respectivamente, Provenance se diseñó para rastrear cualquier tipo de producto, a lo largo de cada parte de su ciclo de vida.

Los tres utilizan la inmutabilidad de Blockchain para registrar información sobre el viaje de sus productos, pero Provenance es el primero en crear un sistema en el que todo el historial de un producto puede rastrearse completamente desde el productor hasta el consumidor, brindando actualizaciones en cada paso, dónde está, quién lo tiene y por cuánto tiempo.

Ejemplo de sistemas de cadenas de suministro en el sector farmacéutico

En el caso de las cadenas de suministro la implementación de la tecnología DLT permite la remoción de intermediarios como agencias de aduanas transfronterizas; esta tecnología garantiza, que las facturas digitales, certificados de autenticidad y todo aquel documento que en la actualidad esté relacionado con este tipo de procesos se convierta en un activo digital, bajo el cual se garantice que la información no se modifique en ningún momento a lo largo del proceso. Consideremos como ejemplo un lote de medicamentos que se producen y se envían desde la fábrica, al momento de iniciar el proceso se genera el artúiculo y se construye una cadena de bloques en DLT/Blockchain que permitirá tener el lote de producción, este lote se marca con la hora y se coloca en la DLT/Blockchain, se autentica y se marca de nuevo en cada punto intermedio (marcando desde las compras a proveedores hasta las ventas y los clientes que la adquieren), desde que comienza el proceso de despacho y transporte a que haya lugar, hasta llegar al destinatario final. En este tipo de procesos, se recupera la confianza y credibilidad en el sector público.

Esta propuesta, que combina seguimiento de la cadena de suministro y hacer pública la información a sus usuarios, la viene liderando el proyecto británico llamado Provenance (Every product has a story). DLT/Blockchain pueda ver en tiempo real, el estado actual del proceso, rompiendo la barrera de la confianza y capturando clientes que cada día valorarán más los productos de empresas éticas y transparentes. Esta propuesta, que combina seguimiento de la cadena de suministro y hacer pública la información a sus usuarios, la viene liderando el proyecto británico llamado Provenance (*Every product has a story*).

¿Quién lo está implementando?

Maersk, la empresa de envíos más grande del mundo está utilizando la tecnología DLT/Blockchain para monitorizar todos los productos que transporta y de esta forma poder ofrecer la información a los diferentes actores de la cadena de suministro. Para ello se ha desarrollado, en colaboración con IBM, una herramienta que permite que cada actor de la cadena de suministro haga un seguimiento de su envío; gracias a ello es posible saber dónde se encuentra el contenedor y el estatus de sus documentos, con lo cual se puede reducir considerablemente la carga de papeleo para los transportistas y permitir que los agentes de aduanas y los clientes visualicen dónde se encuentra la mercancía en todo momento.

5.3. Sector musical

La plataforma de "música abierta" de Ujo Music está diseñada para concentrar las identidades y los negocios de los artistas en sitios web de artistas, dónde se comercializa su contenido, las regalías se distribuyen rápidamente a través de la moneda digital Bitcoin y se evitan los enredos tradicionales de la industria (Milt, 2016).

A continuación, se demostrará en la Tabla 10, que el sector musical también tiene oportunidades, desafíos e interesados (Stakeholders) para poder realizar un buen ejercicio o beneficiarse por medio del DLT/Blockchain:

Tabla 10 Implementación de la tecnología DLT/Blockchain en el sector musical

OPORTUNIDADES	DESAFÍOS	INTERESADOS
Nuevos modelos de negocio que se basan en servicios directos al consumidor, en tiempo real y de pago según uso. Conectar directamente a los productores de contenido (incluidos los artistas) y los consumidores, y alinear el consumo de medios con el precio pagado Simplificación de los pagos de regalías, mejor protección de datos y costos reducidos para la protección de la propiedad intelectual. Reducción de la fragmentación en la distribución de contenidos y recaudación de ingresos.	Falta de un único formato de datos interoperable. Múltiples bases de datos de contenido y fragmentación resultante. Proliferación del mismo contenido en múltiples plataformas de transmisión (no interoperables). Resistencia de los intermediarios actuales y posible pérdida de puestos de trabajo.	Distribuidores de música. Plataformas de transmisión: Spotify, Apple Music, entre otros. Plataformas de descarga de música: Apple iTunes, Google Play. Grabar etiquetas / editors: Universal Music Group, Sony Music Entertainment, Warner Music Group. Músicos y artistas (Grupos o solistas). Propietarios y distribuidores de catálogos de música existentes. Usuarios finales / organizaciones que representan los intereses y derechos de los usuarios finales.

6. Recomendaciones para la implementación de políticas públicas

Considerando las ventajas identificadas en capítulos anteriores de este documento, la presente sección ofrece recomendaciones en términos del marco técnico, político y regulatorio necesario para llevar a cabo la implementación de políticas relacionadas con la tecnología.

Experiencias desarrolladas y lecciones aprendidas: de las experiencias en los siguientes cuatro países: Emiratos Árabes Unidos, Estonia, China y Unión Europea; se identifican beneficios y casos de uso de la tecnología relacionados con el sector público. Estas experiencias y casos de uso permiten identificar retos, oportunidades y recomendaciones sobre la viabilidad de la implementación de la tecnología DLT en el sector público en Colombia, las cuales se consolidan en la sección 6.3.

Posteriormente, se realiza una priorización de estas recomendaciones para plantear una hoja de ruta que permita el aprovechamiento de la tecnología desde el sector público en el mediano plazo. La sección concluye con una síntesis de las recomendaciones para la formulación, coordinación y evaluación de políticas públicas relacionadas con la tecnología, así como los requisitos para la implementación de la misma.

6.1. Experiencias de formulación de políticas públicas en otros países del mundo

Diferentes países alrededor del mundo se han preocupado por explotar los beneficios del uso de la tecnología DLT en el sector público. En la Tabla 11**¡Error! No se encuentra el origen de la referencia.**, se presentan los avances particulares de seis países, que se han destacado en la implementación de la tecnología desde el gobierno.

Tabla 11 Evidencias de las experiencias internacionales Blockchain

PAÍS	AVANCE
Estonia 	• Empezó a incursionar en DLT en 2008, antes que esta tecnología se convirtiera en tendencia, incluso antes que Satoshi Nakamoto inventara al Bitcoin. Esta iniciativa surgió como respuesta al ataque cibernético que le afectó en 2007 el cual dejó sin conexión en los sitios web de los servicios estatales. Esto desencadenó que el país priorizará la seguridad de los datos. • El uso de identificadores de firma sin clave (Keyless signature identifiers) ha permitido ampliar la oferta de servicios de gobierno en línea, así como la protección de la información. • Desde 2012 se emplea para proteger datos nacionales, servicios en línea y dispositivos inteligentes, tanto en el sector público como en el privado. Desde este año, la tecnología se emplea en los registros de información de los sistemas de salud, jurídico, legislativo, de seguridad y comercial. • Se proyecta ampliar su uso a los ámbitos de medicina personal, ciberseguridad y embajadas.
China 	• Se introduce la tecnología en 2016 con un proyecto denominado "El área experimental y comprensiva del Big Data en la provincia de Guangdong". • Se ha desarrollado un sistema de identidad digital con autenticación y firma digital que permite solventar problemas de crédito y se ha empleado la tecnología para hacer seguimiento a la calidad en los procesos de producción, transporte y mercadeo en 73 mercados de productos agrícolas.
Emiratos Árabes Unidos 	En 2018 el país lanzó la estrategia UAE Blockchain Strategy con la cual espera utilizar la tecnología para el desarrollo del 50% de las transacciones del gobierno a nivel federal, ahorrando 3 billones de dólares al mes por transacciones y documentos en papel, 77 millones de horas de trabajo y reduciendo los documentos del Estado en 389 millones.
Países de la Unión Europea 	• La comisión europea lanzó el Observatorio de Blockchain de la Unión Europea en febrero de 2018. Este observatorio permite resaltar los desarrollos más importantes de la tecnología, promoviendo la masificación de actores involucrados en actividades de Blockchain. • La comisión europea manifestó que desea construir sobre iniciativas que ya están desarrollándose a nivel nacional para desarrollarlas superando cada vez más fronteras. Para ello, se proponen financiar proyectos de Blockchain en hasta 340 millones de euros a 2020.

PAÍS	AVANCE
Estados Unidos 	• En el país las autoridades locales reconocen el potencial de las tecnologías DLT (Blockchain y Contratos Inteligentes) en la prestación de servicios públicos. • La iniciativa pionera se implementó en 2016 en el estado de Delaware. • Para finales de 2018 otros estados lo han secundado al implementar este tipo de tecnología para la transformación de los servicios públicos y privados, por ejemplo: Illinois, Virginia Occidental y New York
Canadá 	• El Gobierno de Canadá, en el segundo semestre del 2018, logró implementar exitosamente la blockchain de Ethereum para la administración transparente de subsidios y otras contribuciones del gobierno, como había declarado en enero del mismo año. • Este país es uno de los que mayor interés ha mostrado en el desarrollo de la tecnología de criptoactivos para sectores tan diversos como el agrícola y la regulación de las ICO, así como también ha tenido en consideración emitir monedas digitales.

Impactos sociales positivos:

- En Estonia se reconoce que los registros del sistema de salud basados en Blockchain han permitido identificar el uso indebido de información, evitando perjuicios mayores a la salud de un individuo por prescribir la medicina o dosis errónea.

- En China se identifican como beneficios de la implementación de la tecnología las mejoras en la cantidad y calidad de servicios del gobierno, la mayor transparencia y accesibilidad de la información, el desarrollo de intercambio de información entre organizaciones y el aporte a la construcción de un sistema crediticio individual.

6.2. Identificación de estándares de la tecnología y necesidades regulatorias

De las experiencias internacionales presentadas al inicio de esta sección se derivan las siguientes lecciones aprendidas que constituyen las bases para la implementación de la tecnología DLT en el Estado:

Se requiere establecer una plataforma general de aplicación de la tecnología, desarrollando estándares de administración para promover el gobierno digital soportado en la tecnología. La principal dificultad en el desarrollo de esta acción consiste en la alta inversión inicial requerida para el desarrollo de una plataforma única de gobierno digital soportada en la tecnología. Para reducir estos costos será necesario clarificar conceptos básicos, procesos y estándares para mejorar el conocimiento sobre la tecnología, unificar la interfaz de la programación para el desarrollo de la plataforma y promover la interoperabilidad de múltiples sistemas soportados en la tecnología y perfeccionar los procesos operativos requeridos.

Blockchain provee una forma efectiva de mejorar la eficiencia en los servicios del gobierno, pero estandarizar el sistema de manejo, procesos y responsabilidades de la aplicación será necesario para su promoción. Para ello se deben realizar discusiones con enfoque interdisciplinario sobre las bases para la implementación y el mantenimiento de largo plazo de plataformas del gobierno basadas en la tecnología. Por lo anterior, la experticia de instituciones gubernamentales, organizaciones de tecnología y el sector público asociado, es fundamental en dichas discusiones.

Tabla 12 Retos para la implementación de la tecnología DLT en el sector público

RETOS IDENTIFICADOS PARA LA IMPLEMENTACIÓN DE LA TECNOLOGÍA EN EL SECTOR PÚBLICO	IDENTIFICADOR
Eliminar intermediación	Comisión Europea
Aumentar confianza	Comisión Europea, China

RETOS IDENTIFICADOS PARA LA IMPLEMENTACIÓN DE LA TECNOLOGÍA EN EL SECTOR PÚBLICO	IDENTIFICADOR
Aumentar seguridad	Comisión Europea, China
Aumentar trazabilidad	China

6.3. Planteamiento de hoja de ruta recomendada para el aprovechamiento de la tecnología

Basados en "*Technology Roadmapping in Canada: A development Guide*", y adaptando los conceptos, no a una industria, sino a una tecnología (específicamente DLT/Blockchain), se procede a realizar una propuesta metodológica para el diseño de una hoja de ruta, que primero que todo, debe ser entendida como un proceso y no como una actividad; es decir que la hoja de ruta (Roadmapping) no consiste en una lista de chequeo o en una fórmula a seguir para obtener un resultado específico, sino que está definida como un proceso iterativo que permite identificar los principales aspectos que deben ser tenidos en cuenta para maximizar las probabilidades de apropiar adecuadamente una tecnología en un sector específico de la economía.

Partiendo de este hecho se procede entonces a utilizar los elementos enunciados en "*Technology Roadmapping in Canada: A development Guide*" y a adaptarlos al caso colombiano para obtener una primera aproximación a una hoja de ruta para la adopción de la tecnología DLT/Blockchain en el país[20].

Misión

Generar escenarios sociales y productos tecnológicos que promuevan y utilicen las tecnologías DLT/Blockchain en la gestión pública.

Visión

Ser un país líder y reconocido en el contexto internacional, por el uso de tecnologías DLT/Blockchain en la gestión pública, generando así confianza en la interacción gobierno ciudadanía.

[20] La hoja de ruta está planteada con el objetivo de promover el uso productivo de las tecnologías DLT/Blockchain en el sector público en Colombia, partiendo del hecho de que actualmente el país no se encuentra en capacidad de producir esta tecnología por su propia cuenta, como lo evidencia la revisión de SCOPUS y Google Scholar planteada en la sección 4.5, donde se evidencia la poca producción científica al respecto y más aún cuando la mayoría de las investigaciones están relacionadas con una sola aplicación de esta tecnología (las criptomonedas).

Objetivo del proyecto, metas y resultados esperados

Generar aplicaciones tecnológicas basadas en DLT/Blockchain con el fin de facilitar el intercambio ciudadano de recursos que posean valor social o económico en un entorno confiable.

Alcance de las condiciones del mapa de ruta

- Ser un país líder en la implementación de DLT/Blockchain en el sector público en un lapso de 5 años, en aras de mejorar la transparencia, confianza y optimizar procesos en los sectores gubernamentales.

- Adaptar y desarrollar aplicaciones informáticas haciendo uso de la tecnología DLT/Blockchain en el sector público que permita optimizar los procesos al interior de los diferentes entes gubernamentales.

1. La industria actual: sus productos, clientes, proveedores y procesos

Teniendo en cuenta que se ha restringido el mapa de ruta al sector público, es importante entonces entender el ecosistema de DLT/Blockchain para este sector específico y una fuente relevante de información al respecto es el documento desarrollado por Deloitte University Press, "*Will Blockchain Transform the Public Sector?*", donde muestra (Figura 35) por ejemplo los recientes desarrollos oficiales de parte de gobiernos alrededor del mundo en el uso de la tecnología Blockchain específicamente (en este estudio no se realiza diferenciación entre esta y otras tecnologías DLT).

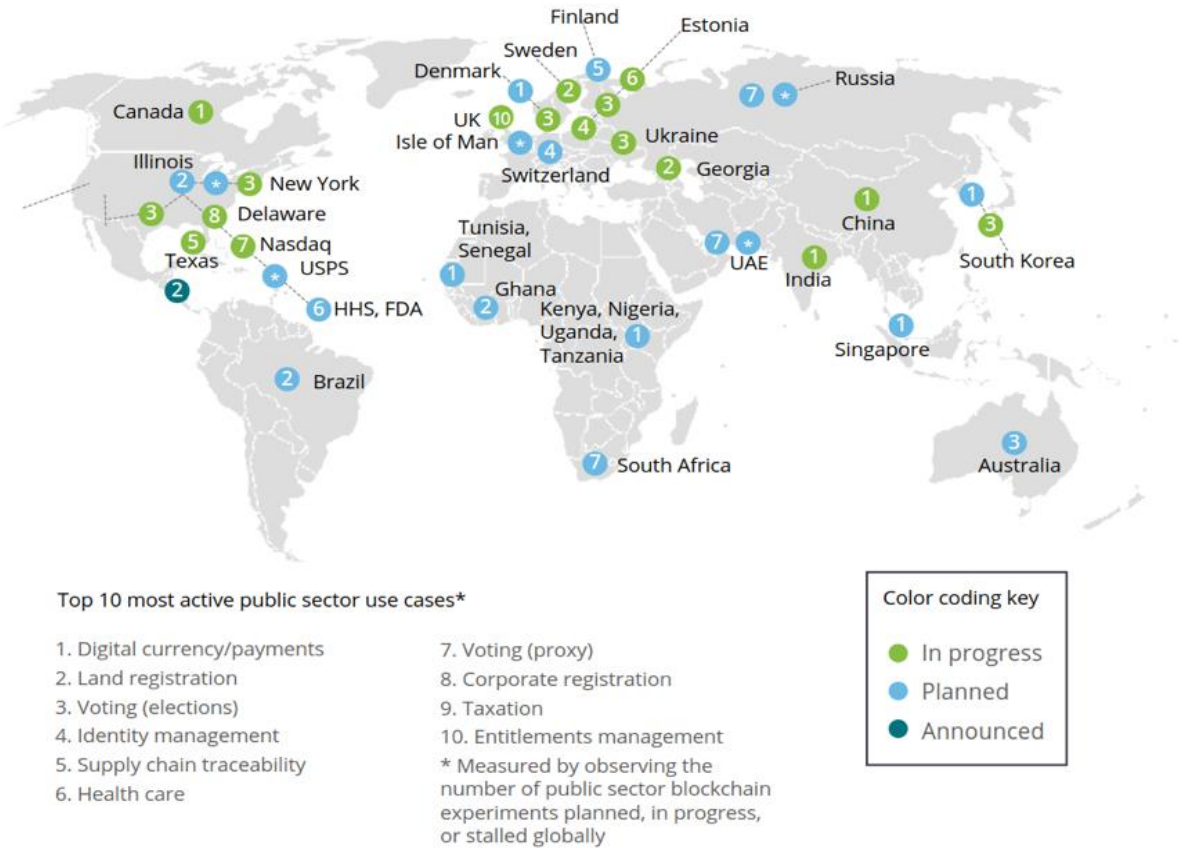

Figura 35 Desarrollos de Blockchain en el sector público[21]

La Figura 35 muestra que principalmente estos desarrollos se están dando en Europa y Norte América (y por lo tanto es en estas áreas donde existe un mayor ecosistema), con una muy poca participación de Latinoamérica.

Ecosistema Blockchain

- Entidades públicas: jefes de las unidades de sistemas, planeación, estadística o interesados en implementar la tecnología DLT/Blockchain; Ministerios, Alcaldías, Gobernaciones o entidades descentralizadas.
- Entidades privadas: agremiaciones, ONGs, cooperativas, Bancos, Bolsa de Valores, emprendedores.
- Congreso de la república: Encargado de generar la legislación necesaria para el correcto funcionamiento de la tecnología DLT/Blockchain en Colombia.
- Ciudadanos: desarrolladores
- Sector académico.

[21] Tomado de Deloitte University Press, "*Will Blockchain Transform the Public Sector?*" (Marzo de 2017)

Los modelos de uso de datos que aquí se desarrollan están asociados a conjuntos de datos abiertos, presentes en el portal www.datos.gov.co que, a partir de herramientas analíticas, generan indicadores asociados a la Transparencia en la Contratación Pública. Estos conjuntos de datos abiertos han sido publicados por las entidades públicas, en el cumplimiento de la Ley 1712 de 2014 y, reposan en el portal de MinTic, permitiendo un acceso público a la información. Aunque existen otras fuentes de datos, que pueden ser accedidas a través de otros mecanismos de recolección de información como Web Scraping, Web Crawling, Robotización de Consultas, entre otras, han sido excluidos de este proceso, ya que no permiten asegurar la implementación de un modelo sostenible en el tiempo, debido a técnicas que limitan su uso como Captcha, Re-Captcha o controles de seguridad que restringen la concurrencia de consultas.

Productos que ofrece DLT/Blockchain

Una de las principales aplicaciones de la tecnología DLT/Blockchain son los contratos inteligentes (smart contracts) que se pueden construir sobre plataformas como Ethereum, NEO o NEM (entre otras) y que están tomando el protagonismo actualmente.

Si bien en el capítulo 5 se trataron temas generales sobre las aplicaciones de DLT/Blockchain en diferentes sectores de la economía, en esta sección es importante resaltar y mencionar aquellos casos de soluciones específicas para el sector público, que están relacionadas con las áreas mostradas en la Figura 36 como las siguientes:

Impactos de DLT/Blockchain

- En el sector financiero, la tecnología DLT/Blockchain permite agilizar las transacciones, estas se pueden realizar a cualquier hora y en cuestión de minutos, reduciendo los costos de las mismas al eliminar intermediarios.
- En el sector salud, el desarrollo de sistemas de información desarrollados sobre plataformas DLT/Blockchain optimiza los tiempos de respuesta del ecosistema.
- En procesos de administración pública, vuelve más transparentes los procesos y la administración pública.
- En proyectos sociales, la transparencia permite verificar el buen uso de los recursos utilizados por empresas sociales, lo que da mayor confianza a los donantes.

Tendencias del mercado y proyecciones

Los nuevos desarrollos y tendencias del mercado están enfocados en desarrollar aplicaciones que permitan:

- Nuevos flujos de ingresos y modelos de negocio basados en registros de datos de salud del paciente.
- Acceso y verificación de datos en tiempo real.

- Uso de contratos inteligentes para desarrollar automáticamente el cumplimiento legal y regulatorio.
- Reducción del fraude en transacciones gubernamentales.
- Reducir los costos de transacción a través de la desintermediación.
- Permitir que los pacientes conserven el control sobre los datos individuales.
- Importancia para la protección de la propiedad intelectual y el registro de datos de las cadenas de suministro.
- Mejorar la eficiencia de la distribución de medicamentos. Reducir la falsificación.
- Conectar directamente a los productores de contenido (incluidos los artistas) y los consumidores, y alinear el consumo de medios con el precio pagado.
- Simplificación de los pagos de regalías, mejor protección de datos y costos reducidos para la protección de la propiedad intelectual.

Limitaciones relevantes

- Como ya vimos en la sección 4.5, la principal limitación para implementar la tecnología DLT/Blockchain en Colombia es la falta de conocimiento; bajo la cual los procesos de apropiación y aplicación del conocimiento se hacen mucho más extensos y no se cuenta con la capacidad instalada para llevar los procesos a gran escala.
- Desde el punto de vista técnico, la escalabilidad y la convergencia son limitantes a la hora de implementar la tecnología DLT/Blockchain.
- Desde el punto de vista legal, Colombia no cuenta con una legislación que permite la incorporación de la tecnología en el sector público.

2. Necesidades técnicas y capacidades

Productos deseados

Dada la importancia que está adquiriendo la tecnología DLT/Blockchain en el mundo, se hace necesario citar algunos de los productos más importantes, que podrían transformar el sector público y las entidades gubernamentales en Colombia, los productos se muestran en la sección **5.1 Gobierno** de la presente guía.

Barreras y brechas

En la implantación de la tecnología DLT/Blockchain existen barreras y brechas de tipo conceptual-cultural y tecnológicas la cuales describiremos a continuación.

Barreras de tipo Conceptual-Cultural

Desconocimiento de las posibilidades de uso en el sector público.

- Para identificar un activo digital se requiere reconocer dónde radica el valor social o económico para establecer “el activo” y cómo generar confianza en que este valor puede residir en un formato digital. Se considera una barrera conceptual porque identifica que el valor no es un asunto trivial y se considera cultural porque para un ciudadano es más confiable un documento que puede guardar en su escritorio.
- Al momento de plantear una arquitectura DLT puede requerirse de los nodos mineros, los cuales realizan su trabajo por un incentivo, en el caso de Bitcoin el incentivo está claro y son criptomonedas en otras aplicaciones como un banco de tiempo o en una cadena logística la recompensa de los nodos mineros ¿tendrá que ser siempre dinero?, o ¿cómo puedo motivar este esfuerzo computacional?
- Generación de usuarios, generar confianza e incrementar la usabilidad de una plataforma DLT siempre es una barrera cultural.

Barreras tecnológicas

- Pocos profesionales capacitados en la implantación de aplicativos DLT.
- Los tiempos de respuesta en una transacción.
- La escalabilidad de la solución.

Brecha Conceptual-Cultural

- El nivel de apropiación de la tecnología en el país es bajo, comparado con países como el Reino Unido.

Brecha Tecnológica

- Existen diferencias entre las posibilidades de implementación de la tecnología entre grandes ciudades y territorios nacionales o municipios de 5a y 6a categoría.

3. Necesidades técnicas y capacidades

Para superar las barreras y brechas del conocimiento es indispensable generar procesos de transferencia del conocimiento en el ecosistema DLT/Blockchain.

Estrategia de desarrollo de capacidades

Evaluación de las necesidades que se requieren para implementar DLT

Como ya se mencionó en la **sección 4.5**, una de las principales limitaciones es la falta de conocimiento de la tecnología, identificando un mínimo número de publicaciones relacionadas con DLT/Blockchain, donde las más antiguas datan del año 2016 y donde además algunas tratan directamente el tema de criptoactivos o de bitcoin.

Lo anterior nos permite concluir que el nivel de desarrollo de la tecnología en el país, desde el punto de vista académico es muy incipiente. Así que cualquier desarrollo o implementación de esta tecnología a nivel país debe darse replicando algunos de los esfuerzos del gobierno por desarrollar pilotos en la materia mediante la transferencia de tecnología y de conocimiento con aliados estratégicos que tengan una mayor madurez en el desarrollo de soluciones basadas en DLT/Blockchain.

Recomendaciones de mejoras de programas para las habilidades necesarias para implementar DLT/Blockchain

Ante la falta de la existencia de una masa crítica con las capacidades para realizar los desarrollos necesarios lo más sensato es promover programas de transferencia de conocimiento basados en la tecnología Blockchain, que permita a los actores del ecosistema adquirir las capacidades relevantes para desarrollar sistemas de información basados en Blockchain contribuyendo a la solución de problemas del sector público.

4. Puntos de decisión y cronograma

Para el desarrollo de un cronograma tentativo que permita la implementación de la tecnología DLT/Blockchain en el sector público y que permita a Colombia ser un país líder en la región en la implementación y desarrollo de aplicaciones sobre esta tecnología se proponen las siguientes actividades:

Actividad #1: Capacitación al ecosistema DLT/Blockchain

Al ser una tecnología emergente, se requiere capacitar a desarrolladores, emprendedores de las TIC y empleados del sector público respecto a la tecnología y su implementación.

Actividad #2: Levantamiento de requerimientos funcionales

Levantamiento de requerimientos que permitan la eficaz implementación de la tecnología DLT/Blockchain en el sector público.

Actividad #3: Publicación de requerimientos

Al ser una tecnología emergente se requiere que todos los actores relacionados con el ecosistema conozcan los requerimientos bajo los cuales se implementará la tecnología DLT/Blockchain, de tal manera que se desarrolle un trabajo colaborativo.

Actividad #4: Análisis y diseño

Diseño de los casos de uso necesarios para la implementación de la tecnología DLT/Blockchain en el sector público.

Actividad #5: Desarrollar la aplicación DLT

Implementación de un sistema de información, basado en la tecnología DLT/Blockchain en el sector público.

Actividad #6: Validación

A partir de los resultados obtenidos, se desarrolla un proceso de mejoramiento que permita optimizar la aplicación.

Actividad #7: Evaluación de impacto

Los actores del ecosistema Blockchain desarrollaran actividades de evaluación e impacto, que permita a los ciudadanos y entes gubernamentales conocer e implementar la tecnología Blockchain en el sector público.

Cronograma tentativo

Tabla 13 Cronograma tentativo

Implementación de la tecnología DLT/Blockchain en el sector público										
Cronograma de actividades										
Actividad	Semestre									
	1	2	3	4	5	6	7	8	9	10
Capacitación al ecosistema DLT/Blockchain										
Levantamiento de requerimientos funcionales.										
Publicación de requerimientos										
Análisis y diseño										
Desarrollar la aplicación DLT										
Validación										
Divulgación										

A continuación, se presenta un diagrama de flujo que describe los pasos metodológicos que se deben llevar a cabo para la implementación y desarrollo de tecnología DLT.

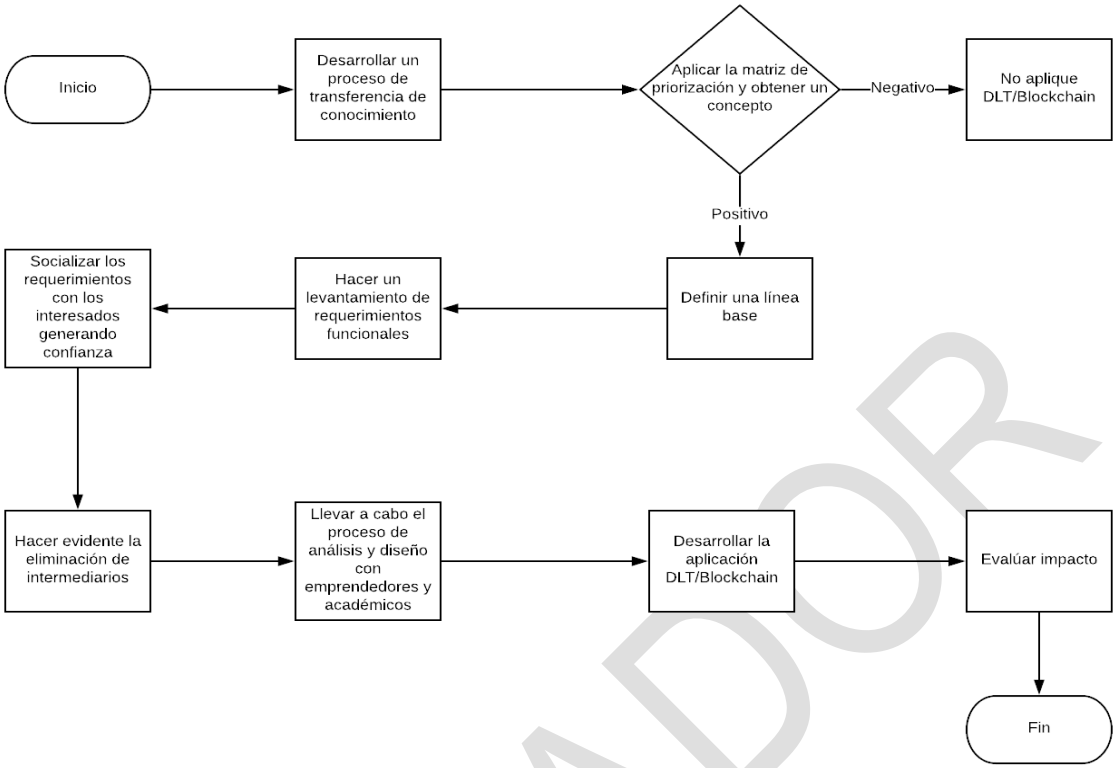

Figura 36 Metodología para la implementación de DLT/Blockchain

5. Conclusión

- La tecnología DLT/blockchain elimina los intermediarios y permite trabajar solo con activos digitales.
- Los contratos inteligentes emulan la lógica de las cláusulas contractuales.
- Los contratos inteligentes permiten efectuar transacciones "sin confianza", monitorear y ejecutar bilateralmente a través de una red digital sin necesidad de un intermediario externo de confianza.
- Los procesos de cadenas de suministros garantizan un eficaz seguimiento a los productos, minimizando la falsificación y asegurando que el cliente obtenga sus productos en óptimas condiciones.

6. Recomendaciones

- Generar un marco normativo, para que la tecnología DLT/Blockchain pueda ser implementada en el sector público.
- Desarrollar procesos de transferencia de conocimiento que permitan al ecosistema DLT/Blockchain interiorizar la tecnología y desarrollar aplicaciones en el sector público.
- Las personas que participan en un proyecto de DLT/Blockchain deben comprender la tecnología o al menos sus implicaciones.

- Con DLT/Blockchain no puede desarrollar procesos de almacenamiento de altos volúmenes de información.
- Si la solución propuesta no busca o no requiere administrar de manera cuidadosa el intercambio de valor de un activo digital, entonces quizá una tecnología diferente a DLT/Blockchain pueda ser una mejor solución.

6.4. Recomendaciones sobre cómo implementar la tecnología en caso de una decisión positiva al respecto

Desarrollar un mapa de ruta que permita definir los aspectos fundamentales a ser considerados para que Colombia sea un país pionero en la región en cuanto a la adopción de tecnologías basadas en DLT/Blockchain a partir del documento planteado por el WEF "*Blockchain Beyond the Hype A Practical Framework for Business Leaders*", creando una matriz de priorización de proyectos a partir del cumplimiento de las condiciones planteadas en dicho documento. Al ser una matriz de priorización, la calificación como valor absoluto, no tiene un significado especial, sino que un caso de uso que obtenga una puntuación (por ejemplo) de 80 debería ser priorizado sobre uno que haya obtenido una de 70.

Así las cosas, el primer paso es identificar aquellos procesos o procedimientos que cumplen características fundamentales o habilitantes (y por ende que no asignan puntaje) para realizar proyectos basados en esta tecnología, que se citan a continuación:

Tabla 14 Identificación de características fundamentales para implementar DLT/Blockchain

ÍTEM	CONDICIÓN	HABILITANTES
1	Se está trabajando con activos digitales	x
2	Se está tratando de remover intermediarios o agentes comerciales	x
3	Se puede crear un registro permanente del activo digital	x

1. Se está tratando de remover intermediarios o agentes comerciales

Por motivos de contexto de los procesos es importante entender si la solución que se pretende implementar busca o requiere la remoción de intermediarios o agentes comerciales (que pueden estar incluso dentro de la misma entidad) como parte fundamental de su desarrollo.

Este aspecto es de vital importancia, puesto que, por sus características, incluso las tecnologías de DLT/Blockchain han sido denominadas de manera genérica como tecnologías de desintermediación.

2. Se está trabajando con activos digitales

Por sus características nativas digitales, las tecnologías DLT/Blockchain tiene la capacidad de trabajar de una manera eficiente sobre activos digitales que no pueden ser utilizados como bienes de capital, es decir que no pueden ser transformados en otros activos.

3. Se puede crear un registro permanente del activo digital

La necesidad de poder crear un registro permanente del activo digital es la característica fundacional de una solución basada en la tecnología DLT/Blockchain, puesto que este registro es el que se convertirá en la cadena de bloques o libro maestro de la solución desarrollada.

Hasta aquí se han descrito entonces los 3 principales elementos (habilitantes) con los cuales debe contar una solución basada en tecnologías DLT/Blockchain. Ahora se pasa a la descripción de los aspectos puntuables, que al ser preguntas que se pueden responder con un sí o un no, asignan o 0 o el puntaje máximo (es decir que no hay valores intermedios). Esto además ayuda a reducir la subjetividad de tener que diferenciar un 4 de un 5 en un caso de uso específico.

Tabla 15 Matriz de priorización de proyectos basados en DLT/Blockchain[22]

ÍTEM	CONDICIÓN	PUNTAJE
1	No se requiere alto desempeño y transacciones rápidas (en milisegundos)	10
2	No se requiere almacenar amplios volúmenes de datos no transaccionales como parte de su solución	10
3	No necesita contar con una contraparte confiable	20
4	Está manejando relaciones contractuales o intercambio de valores	20
5	Requiere acceso de escritura compartido	10
6	Los colaboradores no pueden confiar entre ellos	10
7	Necesita controlar las funcionalidades	10
8	Las transacciones deben ser públicas	10

[22] Elaboración propia basada en Blockchain Beyond the Hype A Practical Framework for Business Leaders, Dr. Catherine Mulligan, CREDIT: Cryptocurrency Effects in Digital Transformations (EP/N015525/1).

1. No se requiere alto desempeño y transacciones rápidas

El estado actual de la tecnología DLT/Blockchain plantea como uno de los principales cuellos de botella los tiempos de procesamiento y la escalabilidad de las soluciones. En este caso se hace referencia al primero de los problemas, y es el tiempo que toma en confirmar las transacciones, motivo por el cual en la actualidad no es deseable implementar soluciones que posteriormente en la práctica requerirán tiempos de procesamiento en el orden de los milisegundos.

2. No se requiere almacenar amplios volúmenes de datos no transaccionales

Ahora, en materia de escalabilidad, no es deseable utilizar la tecnología DLT/Blockchain para ser considerada como un sistema de almacenamiento de datos no transaccionales.

3. No necesita contar con una contraparte confiable

En este aspecto es importante revisar de manera explícita si existen procedimientos o regulación que impidan o que comprometan el futuro despliegue de una posible solución basada en DLT/Blockchain y que tenga como fuente fundamental el cumplimiento de regulaciones o de estándares, por muy buena que pueda ser la solución. Por ejemplo, en el caso de la creación de un criptoactivo que represente una moneda de curso legal, es necesario involucrar y contar con la participación de las entidades que regulan la materia en el país (Banco de la república, URF y Superintendencia Financiera).

4. Está manejando relaciones contractuales o intercambio de valores

Si existe un valor intrínseco en las transacciones a ser manejadas por una solución DLT/Blockchain, entonces también existe un incentivo a que un agente malintencionado pueda tratar de acceder a este “valor” y obtener una ganancia.
Por lo anterior, si la solución propuesta no busca o no requiere administrar de manera cuidadosa el intercambio de valor de un activo digital, entonces quizá una tecnología diferente pueda ser una mejor solución.

5. Requiere acceso de escritura compartido

Es importante recordar la naturaleza descentralizada de DLT/Blockchain, por lo que es posible pensar en mecanismos donde se requiera que algunos (o todos) de los miembros de la red puedan realizar y registrar transacciones. Si este no es el caso, entonces es probable que otra tecnología (centralizada) pueda ser una mejor solución.

6. Los colaboradores no pueden confiar entre ellos

Partiendo de nuevo de la naturaleza descentralizada de DLT/Blockchain y del hecho de que existe un intercambio de valor en la solución que puede generar incentivos para que un

agente no deseado busque obtener una ganancia, es importante establecer entonces si existe confianza entre los colaborares de la red y sobre si estos se conocen entre sí. Si existe confianza o si existen mecanismos que obliguen a los colaboradores a actuar de una manera honesta, entonces otra tecnología puede ser una mejor solución.

Hasta este punto se han evaluado las características de la solución y su alineación con el potencial uso de la tecnología DLT/Blockchain, así que ahora se procede a evaluar algunas de las características esperadas de su configuración y funcionalidades internas.

7. Necesita controlar las funcionalidades

Si es necesario que sobre la solución desarrollada se tomen decisiones sobre sus funcionalidades (aquellas relacionadas con la configuración interna de la DLT/Blockchain) como la distribución, ubicación y número de nodos, o el mecanismo o algoritmo de consenso, entre otros, entonces es necesario que el despliegue y desarrollo se haga sobre una DLT/Blockchain privada.

Si las funcionalidades internas de la DLT/Blockchain son irrelevantes para la solución, entonces una DLT/Blockchain púbica puede ser una excelente alternativa.

8. Las transacciones deben ser públicas

Si las transacciones almacenadas en la DLT/Blockchain deben ser visibles y accesibles para todo el mundo, entonces una solución púbica tiene más sentido.

En este punto es importante recordar que también existen los ambientes híbridos, donde se tiene una mezcla entre una DLT/Blockchain privada y una pública, para por ejemplo garantizar el control sobre las funcionalidades sin comprometer la publicidad de las transacciones.

Entonces, dentro del mapa de ruta que busca que Colombia sea un país líder en la adopción de soluciones basadas en esta tecnología es de suma importancia contar con una herramienta que permita brindar un mecanismo objetivo para la priorización de potenciales proyectos que se puedan implementar mediante el desarrollo de soluciones basadas en DLT/Blockchain, minimizando su tasa de fracaso al considerar no solamente los aspectos técnicos, sino también de procesos y de regulación asociados a los mismos.

De otro lado es importante mencionar que la matriz desarrollada debe ser actualizada constantemente debido al rápido avance de la tecnología, puesto que, por ejemplo, en 6 meses, la escalabilidad de la tecnología DLT/Blockchain deje de ser una limitante en los proyectos y en consecuencia, la respuesta al punto 4 puede cambiar.

6.5. Ejemplos para el uso de la matriz de priorización

Desde el punto de vista del usuario final. Para la entidad, un intermediario puede ser un funcionario público; un tercero de confianza puede ser el director de la misma, etc.

Inicialmente es importante recordar que la matriz de priorización provee un contexto desde el punto de vista técnico sobre la pertinencia y posible éxito de una solución basada en DLT/Blockchain para una problemática específica. Esta matriz, es un punto de partida, y como tal debe ser acompañada de otros aspectos (no necesariamente técnicos) como estimaciones presupuestales, implicaciones de política pública entre otros, para poder determinar con una mayor precisión, los posibles efectos del desarrollo de algunas de las potenciales soluciones propuestas.

Adicionalmente, antes de iniciar el proceso de evaluación de la matriz, se requiere definir de manera el punto de referencia desde el cual se está realizando la evaluación, ya que esto afecta de manera significativa los resultados.

Por ejemplo, para el primer ítem de la matriz sobre si se está buscando remover un intermediario, para una entidad que esté pensando en implementar un sistema de aprobaciones de comisiones y viáticos, la persona encargada de este trámite dentro de la Entidad es el intermediario, y la persona encargada de aprobar la solicitud es la “contraparte confiable”.

Debido al objetivo principal de esta guía, es importante aclarar que el punto de referencia por defecto está asociado a un ciudadano en general.

Ahora, para mostrar el uso (y la utilidad) de la matriz, se plantean 3 escenarios hipotéticos, sobre los cuales se realizarán los respectivos análisis:

1. Solución de titulación de propiedades (con oficina de registro).
2. Solución de titulación de propiedades (sin oficina de registro).
3. Solución de certificación de notas escolares.

1. Solución de titulación de propiedades (con oficina de registro)

Uno de los casos de uso más frecuentes de DLT/Blockchain para el sector público ha sido planteado como una solución que permita garantizar la no alteración y la originalidad de los títulos de propiedades, partiendo de las reconocidas características de DLT/Blockchain para cumplir con estos dos objetivos.

En este primer caso, se propone entonces un escenario donde los títulos de las propiedades se creen (y se transen) mediante el uso de tecnología DLT/Blockchain, pero donde todavía existe una entidad central (la oficina de registro) que es la única entidad que puede realizar procesos de inserción (o de escritura) en la base de datos.

Se inicia entonces por la revisión de los aspectos habilitantes según la matriz.

Tabla 16 Identificación de características DLT/Blockchain Ejemplo Propiedad de Tierras

ÍTEM	CONDICIÓN	EVALUACIÓN	HABILITANTE
1	Se está tratando de remover intermediarios o agentes comerciales	Actualmente para que las personas puedan demostrar la titularidad sobre una propiedad (bien raíz) se requiere de un tercero de confianza (oficina de registro) quien emite un certificado describiendo las características de la propiedad. Lo que busca el sistema de titulación basado en DLT/Blockchain es que ahora las personas puedan tener el control de sus propiedades y poder demostrar la titularidad de las mismas mediante un sistema informático de acceso público y con información en tiempo real.	Sí
2	Se está trabajando con activos digitales	El activo digital es el título digital.	Sí
3	Se puede crear un registro permanente del activo digital	Sí es posible creara un registro permanente del activo digital.	Sí

Se pasa ahora a los aspectos puntuables.

Tabla 17 Matriz de priorización Ejemplo Propiedad de Tierras

ÍTEM	CONDICIÓN	EVALUACIÓN	PUNTAJE
1	No se requiere alto desempeño y transacciones rápidas (en milisegundos)	No se requiere que, en el momento de realizar un cambio en la titularidad de una propiedad, este se registre en cuestión de milisegundos.	10
2	No se requiere almacenar amplios volúmenes de datos no transaccionales como parte de su solución	No se requiere almacenar volúmenes grandes de datos no transaccionales (como fotos, planos, etc.) como parte de la solución.	10
3	No necesita contar con una contraparte confiable	Actualmente, se requiere contar con una contraparte confiable, que precisamente es la Oficina de Registro.	0
4	Está manejando relaciones contractuales o intercambio de valores	Los títulos de las propiedades tienen un gran valor económico, y al permitir que estas sean transables en una plataforma se configura el intercambio de valores.	20

5	Requiere acceso de escritura compartido	En este caso, una plataforma descentralizada para que las personas puedan intercambiar títulos de propiedades, se requeriría acceso de escritura compartido.	10
6	Los colaboradores no pueden confiar entre ellos	Existe el riesgo de que alguien quiera modificar o acceder a la propiedad de un título de manera maliciosa, por lo cual no existe confianza	10
7	Necesita controlar las funcionalidades	Las funcionalidades de la plataforma no se quiere controlarlas	10
8	Las transacciones deben ser públicas	Las transacciones deben ser públicas.	10
	TOTAL		**80**

2. Solución de titulación de propiedades (sin oficina de registro)

Ahora, para este caso se propone un escenario similar al anterior, pero donde ya no existe una entidad central (oficina de registro) que se encargue de garantizar.

Tabla 18 Identificación de características DLT/Blockchain Ejemplo Titulación de Propiedades

ÍTEM	CONDICIÓN	EVALUACIÓN	HABILITANTE
1	Se está tratando de remover intermediarios o agentes comerciales	Actualmente para que las personas puedan demostrar la titularidad sobre una propiedad (bien raíz) se requiere de un tercero de confianza (oficina de registro) quien emite un certificado describiendo las características de la propiedad. Lo que busca el sistema de titulación basado en DLT/blockchain es que ahora las personas puedan tener el control de sus propiedades y poder demostrar la titularidad de estas mediante un sistema informático de acceso público y con información en tiempo real.	Sí
2	Se está trabajando con activos digitales	El activo digital es el título digital.	Sí
3	Se puede crear un registro permanente del activo digital	Sí es posible creara un registro permanente del activo digital	Sí

Tabla 19 Matriz de priorización Ejemplo Titulación de propiedades

ÍTEM	CONDICIÓN	EVALUACIÓN	PUNTAJE

1	No se requiere alto desempeño y transacciones rápidas (en milisegundos)	No se requiere que en el momento de realizar un cambio en la titularidad de una propiedad, este se registre en cuestión de milisegundos.	10
2	No se requiere almacenar amplios volúmenes de datos no transaccionales como parte de su solución	No se requiere almacenar volúmenes grandes de datos no transaccionales (como fotos, planos, etc.) como parte de la solución.	10
3	No necesita contar con una contraparte confiable	Actualmente, se requiere contar con una contraparte confiable, que precisamente es la Oficina de Registro.	20
4	Está manejando relaciones contractuales o intercambio de valores	Los títulos de las propiedades tienen un gran valor económico, y al permitir que estas sean transables en una plataforma se configura el intercambio de valores	20
5	Requiere acceso de escritura compartido	En este caso, una plataforma descentralizada para que las personas puedan intercambiar títulos de propiedades, se requeriría acceso de escritura compartido.	10
6	Los colaboradores no pueden confiar entre ellos	Existe el riesgo de que alguien quiera modificar o acceder a la propiedad de un título de manera maliciosa, por lo cual no existe confianza	10
7	Necesita controlar las funcionalidades	Las funcionalidades de la plataforma no se quiere controlarlas	10
8	Las transacciones deben ser públicas	Las transacciones deben ser públicas	10
	TOTAL		**100**

3. Solución de certificación de notas escolares

En el caso en el que se desee utilizar la tecnología DLT/Blokchain para garantizar la integridad de un certificado de notas de los estudiantes.

Tabla 20 Matriz de priorización Ejemplo Certificación de Notas Escolares

ÍTEM	CONDICIÓN	EVALUACIÓN	PUNTAJE
1	No se requiere alto desempeño y transacciones rápidas (en milisegundos)	No se requiere que, al insertar una nueva nota, esta se vea reflejada en cuestión de milisegundos.	10
2	No se requiere almacenar amplios volúmenes de datos no transaccionales como parte de su solución	No se requiere almacenar volúmenes grandes de datos no transaccionales (exámenes, pruebas, etc.) como parte de la solución.	10

3	No necesita contar con una contraparte confiable	Las notas deben ser ingresadas por los docentes y solamente son válidas con la firma autorizada por la Entidad.	0
4	Está manejando relaciones contractuales o intercambio de valores	No existe una relación contractual o que genere un intercambio de valor.	0
5	Requiere acceso de escritura compartido	No se requiere acceso de escritura compartido (al menos no de manera abierta), ya que solo los docentes tienen la capacidad de registrar información en la solución.	0
6	Los colaboradores no pueden confiar entre ellos	Sí existe confianza entre los colaboradores (ya que son los docentes los encargados de cargar las notas).	0
7	Necesita controlar las funcionalidades	Las funcionalidades de la plataforma no se quiere controlarlas.	10
8	Las transacciones deben ser públicas	Las transacciones deben ser públicas.	10
	TOTAL		**40**

Así las cosas, se puede ver cómo la matriz de priorización de intervenciones puede servir como un instrumento que permita medir de una forma más objetiva los tipos de proyectos que puedan ser desarrollados mediante soluciones basadas en DLT/Blockchain, permitiendo además enfocar los esfuerzos del país para avanzar de una forma más adecuada a convertirse en un líder en la adopción de la tecnología DLT/Blockchain para el sector público.

Esta guía en su totalidad busca acercar a las entidades públicas a una tecnología que ha sido identificada como revolucionaria por el Foro Económico Mundial (WEF), y que además puede aportar de una manera decidida a generar una mayor confianza en el Estado de parte de la ciudadanía y que jugará un papel muy importante desde el punto de vista de la generación de empleo.

Ahora, es importante entonces recordar que la finalidad principal de este documento está orientada a servir de guía a aquellas entidades del sector público que están buscando implementar soluciones basadas en la tecnología DLT/Blockchain, y que como tal presenta de una forma técnica los principales elementos teóricos que fundamentan esta tecnología, permitiendo hacer una diferenciación muy importante entre DLT/Blockchain y las denominadas criptomonedas o criptoactivos (que ha sido uno de los principales retos en cuanto a realizar su distinción para las personas del común y que no tienen una formación técnica), así como los diferentes tipos de DLT/Blockchain y algunos casos de uso representativos que se han dado a nivel internacional.

Adicionalmente otro de los principales mensajes que busca transmitir esta guía es que la tecnología DLT/Blockchain, si bien es una tecnología de propósito general, no debe ser utilizada siempre como la primera opción en el momento de desarrollar o implementar un sistema de información, puesto que como se ha descrito en el documento, esta tiene particularidades que la hacen apta sólo para ciertos tipos de aplicaciones. Además, la decisión de su implementación debe ser pensada de manera cuidadosa y no debe obedecer simplemente a una tendencia tecnológica o de mercado, sino que debe existir un real caso de uso.

Finalmente se trata de que las decisiones sobre si implementar una solución basada en esta tecnología sea lo más objetiva posible y que tenga un sustento técnico que permita sacar el mayor provecho de la futura solución.

Bibliografía

(ILDA), I. L. (s.f.). *ILDA*. Obtenido de ILDA: https://idatosabiertos.org/acerca-de-nosotros/

(ILDA), I. L. (s.f.). *ILDA*. Obtenido de ILDA: https://idatosabiertos.org/en/el-valor-de-los-datos-abiertos-en-america-latina-oportunidades-y-desafios-para-la-innovacion-en-ciudades-abiertas/

Alcaldía de Bogotá. (2018). *Informe de Resultados elección Blockchain.* Bogota.

Argentia, G. d. (s.f.). *Argentina.gob.ar*. Obtenido de Argentina.gol.ar: https://www.argentina.gob.ar/aaip/accesoinformacion/datospublicos

Argentina, G. d. (s.f.). *Datos Argentina*. Obtenido de Datos Argentina: https://datos.gob.ar/

Bach, L., Mihaljevic, B., & Zagar, M. (2018). Comparative analysis of blockchain consensus algorithms. *Rochester Institute of Technology*.

Beikberdi, A., & Song, J. (2015). Trend of centralization in Bitcoin's distributed network. *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 1-6.

Berryhill, J., Bourgery, T., & Hanson, A. (2018). Blockchains Unchained: Blockchain Technology and its use in the public sector. *OECD Working Papers on Public Governance*(28).

BigChain DB GmbH. (2018). *BigchainDB 2.0: The Blockchain Database.* Berlin.

Brasil, G. d. (s.f.). *dados.gov.br*. Obtenido de dados.gov.br: http://dados.gov.br/pagina/sobre

Cachin, C., & Vukolic, M. (2017). Blockchain Consensus Protocols in the Wild. *31st International Symposium on Distributed Computing (DISC)*.

Centro de Innovación Pública Digital. (Diciembre de 2017). Obtenido de Mejoramiento de la seguridad de los servicios del Estado: verificación de identidad e integridad de documentos, a través de Blockchain: http://centrodeinnovacion.gobiernoenlinea.gov.co/es/investigaciones/mejoramiento-de-la-seguridad-de-los-servicios-del-estado-verificacion-de-identidad-e

Chile, C. p. (s.f.). *Consejo para la transparencia*. Obtenido de Consejo para la transparencia: https://www.consejotransparencia.cl/datosabiertos/

Chile, G. d. (s.f.). *datos.gob.cl*. Obtenido de datos.gol.cl: http://datos.gob.cl/about

Commons, C. (s.f.). *Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).* Recuperado el 22 de 4 de 2019, de https://creativecommons.org/licenses/by-sa/4.0/deed.es

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., . . . Wattenhofer, R. (2017). *On Scaling Decentralized Blockchains.* Sin Publicar.

De Angelis, S. (2018). Assesing security and performance of concensus algorithms for permissioned blockchains. *Sapienza Universita di Roma*.

Deshpande, A., Stewart, K., & Lepeti, L. (2017). *Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards.* Londres: British Standards Institution (BSI).

El Espectador. (29 de 08 de 2018). *Así se utiliza blockchain para garantizar la restitución de tierras*. Recuperado el 10 de 09 de 2018, de https://www.elespectador.com/economia/asi-se-utiliza-blockchain-para-garantizar-la-restitucion-de-tierras-articulo-809025

España, G. d. (s.f.). *datos.gob.es*. Obtenido de datos.gob.es: https://datos.gob.es/es/aplicaciones/visor-con-datos-delincuenciales-de-cataluna

España, G. d. (s.f.). *datos.gob.es*. Obtenido de datos.gob.es: https://datos.gob.es/es/aplicaciones/atlas-euskadi-por-areas-pequenas

Garay, J., Kiayias, A., & Leonardos, N. (2015). The Bitcoin Backbone Protocol: Analysis and Applications. *Annual International Conference on the Theory and Applications of Cryptographic Techniques.*

Gastón Concha, A. N. (Marzo de 2012). Gestión Pública. *Datos abiertos: Un nuevo desafío para los gobiernos de la región*. Santiago de Chile: Instituto Latinoamericano y del Caribe de Planificación Económica y Social (ILPES) - CEPAL.

Government Office for Science. (2017). *Distributed Ledger Technology: Beyong Blockchain.* Londres: UK Government Chief Scientific Adviser.

International Organization for Standardization. (2016). *ISO/TC 307 (Blockchain and distributed ledger technologies)*. Recuperado el 13 de 09 de 2018, de https://www.iso.org/committee/6266604.html

ITU-T Focus Group Digital Financial Services. (2017). *Distributed Ledger Technologies and Financial Inclusion.* ITU.

Kiayias, A., & Pangiotakos, G. (2015). Speed-Security Tradeofs in Blockchain Protocols.

Kyoungmin, K., Youngin, Y., Mookyu, P., & Kyungho, L. (2018). *DDoS Mitigation: Decentralized CDN Using Private.* Seoul, Republic of Korea: Korea University.

Liao, T.-C., & Lin, I.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security, 19*(5), 653-659.

Lopez, M. A., & Unda, V. C. (18 de junio de 2018). ¿PÚBLICA, FEDERADA O PRIVADA? EXPLORA LOS DISTINTOS TIPOS DE BLOCKCHAIN. *Banco Interamericano de Desarrollo*.

Map, T. G. (s.f.). *The Great British Toilet Map*. Obtenido de https://www.toiletmap.org.uk/

Mosakheil, J. H. (2018). *Security Threats Classification in Blockchains.* Culminating Projects in Information Assurance.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Sin publicar.

ODI, T. (s.f.). *theodi.org*. Obtenido de Open Data Institute: https://theodi.org/service/tools-resources/data-and-public-services-toolkit/

ODI, T. (s.f.). *theodi.org*. Obtenido de Open Data Institute: https://theodi.org/service/tools-resources/data-and-public-services-toolkit/

Osgood, R. (2016). The Future of Democracy: Blockchain Voting. *COMP116: Information Security.*

RAND Europe. (2017). *Understanding the landscape of Distributed Ledger Technologies/Blockchain: Challenges, opportunities, and the prospects for standards.* Santa Monica, CA: RAND Coorporation.

Slimcoin. (2018). *Slimcoin: A Peer-to-Peer Crypto-Currency with Proof-of-Burn*. Obtenido de Slimcoin: https://bitcointalk.org/index.php?topic=1141676.0

Superintendencia de Industria y Comercio. (2018). *Superintendencia de Industria y Comercio*. Obtenido de Superintendencia de Industria y Comercio: http://www.sic.gov.co/boletines-tecnologicos/blockchain-la-revolucion-de-la-confianza-digital

Swan, M. (2015). *Blockchain: Blueprint for New Economy.* Sebastopol, CA: O'Reilly.

Yli-Huumo, J., Ko, D., Choi, S., & Smolander, K. (2016). *Where is current research on blockchain technology? - A Systematic Review.*


El futuro digital
es de todos
Gobierno
de Colombia
MinTIC