REVISTA TIA

Tecnología, Investigación y Academia -Red Avanzada – RITA
Publicación Facultad de Ingeniería y Red de Investigaciones de Tecnología

Tecnología de registro distribuido (DLT): Características y escenarios de aplicación

Distributed Ledger Technology (DLT): Features and application scenarios

Pava-Díaz, Roberto Albeiro[1] López-Sarmiento, Danilo Alfonso[2] Niño-Vásquez, Luis Fernando[3] Páez-Méndez, Rafael Vicente[4]

Citar este documento:

Pava-Díaz, Roberto Albeiro; López-Sarmiento, Danilo Alfonso, Niño-Vásquez, Luis Fernando; Páez-Méndez, Rafael Vicente. Tecnología de registro distribuido (DLT): Características y escenarios de aplicación. Revista Tecnol.Investig.Academia TIA, ISSN: 2344-8288, 9 (1), pp. 74-90. Bogotá-Colombia.

[1] Ingeniero de Sistemas – Universidad Nacional de Colombia – Colombia. Magister en ingeniería - Ingeniería de sistemas – Universidad Nacional de Colombia – Colombia. Docente – Universidad Distrital "Francisco José de Caldas" – Colombia – rapavad@udistrital.edu.co, roberto.pava@gmail.co. https://orcid.org/0000-0003-0440-892X.

[2] Ingeniero Electrónico - Universidad de Pamplona - Colombia. Doctor en Ingeniería – Universidad Distrital "Francisco José de Caldas" – Colombia, Docente – Universidad Distrital "Francisco José de Caldas" – Colombia – dalopezs@udistrital.edu.co, danilo.lopez.sarmiento@gmail.com, https://orcid.org/0000-0002-6148-3099

[3] Ingeniero de Sistemas – Universidad Nacional de Colombia – Colombia. Magister Matemáticas Universidad Nacional de Colombia – Colombia. M. Sc. Computer Sciencie - The University of Memphis - Estados Unidos. Ph D Computer Sciencie - The University of Memphis - Estados Unidos. Docente – Universidad Nacional de Colombia – Colombia – lfninov@unal.edu.co. https://orcid.org/0000-0003-4703-0007

[4] Ingeniero de Sistemas y Computación - Universidad Católica de Colombia - Colombia. Doctor en Ingeniería Telemática - Universidad Politécnica de Cataluña – España, Docente – Pontificia Universidad Javeriana – Colombia – paez-r@javeriana.edu.co. https://orcid.org/0000-0003-1721-0883

Artículo de reflexión
Fecha de recepción: Noviembre 2020 Fecha de aceptación: Marzo 2021 Vol. 9 No. 1
ISSN: 2344 8288

Resumen

Este artículo describe la Tecnología de Registro Distribuido (DLT, por su sigla en inglés). Se presentan las principales características de DLT cómo son la privacidad, concurrencia y el método de consenso, identificando fortalezas y debilidades de la tecnología. Además, se describen sus dos principales categorías, DLT basado en una cadena de bloques acuñado en la literatura como Blockchain y DLT sin bloques donde su estructura de datos se basa en un grafo acíclico dirigido, denominado usualmente DLT-DAG. Finalmente, se presenta una síntesis de los escenarios de aplicación de esta tecnología agrupados en las siguientes categorías: salud, política y regulación, identidad digital, economía y finanzas, Internet de las cosas y registros de documentos.

Palabras Clave: Blockchain, DLT, DLT-DAG, Tecnología de registro distribuido.

Abstract

This article presents an evolution of Distributed Ledger Technology (DLT) highlighting the differences between its two main categories, DLT based on a blockchain coined in the literature as Blockchain and DLT without blocks where its data structure is based on a graph directed acyclic, usually referred to as DLT-DAG. On the other hand, an analysis of the characteristics of a DLT is carried out, such as privacy, concurrency and the consensus method, identifying strengths and weaknesses. Finally, a synthesis of the application scenarios of this technology is made, grouped into the following categories: health, politics and regulation, digital identity, economy and finance, Internet of things and document records.

Key Words: Blockchain, DLT, DLT-DAG, Distributed ledger technology.

I. Introducción

En un DLT -Distributed Ledger Technology- la información se almacena en una red distribuida y descentralizada de nodos, la cual preserva la veracidad e integridad de los datos mediante la implementación de un algoritmo de consenso. Cada nodo de la red dispone de una copia actualizada del registro histórico de eventos [1],[3].

Dada la estructura de datos que aplique un DLT para enlazar y agrupar las transacciones, se pueden clasificar en dos grupos: (1) DLT con bloque, denominadas en la literatura como Blockchain o DLT-BC y (2) DLT sin bloque, en el cual se vinculan directamente las transacciones entre sí, usualmente en un DAG, y se conocen como DLT-DAG [2]. En las siguientes secciones se presentarán las características de cada uno de estos grupos, DLT-BC y DLT-DAG.

II. Contenido

Tecnología de registro distribuido basada en Blockchain (DLT-BC):

El primer documento técnico que describe la tecnología Blockchain fue titulado "Bitcoin: A Peer-to-Peer Electronic Cash System" [36]. En el año 2008 se presenta este documento en un foro de criptografía, bajo el seudónimo de Satoshi Nakamoto y se especifica un escenario de transferencia directa de valor entre dos personas o entidades, usando dinero digital sin la necesidad de un tercero de confianza para validar y certificar las transacciones.

La integridad y veracidad de la información se logra mediante trabajo colaborativo de los participantes, los cuales ejercen supervisión sobre las transacciones mediante la aplicación de un algoritmo de consenso basado en una prueba de trabajo [37]. Nakamoto define una moneda electrónica -bitcoin- como una cadena de firmas digitales [5], basadas en un sistema de cifrado asimétrico, que se pueden verificar automáticamente sin la necesidad de un tercero de confianza e implementada con un servidor de marcas de tiempo [38] público con el objeto de prevenir una transacción fraudulenta, la cual se presenta cuando un usuario intenta transferir un mismo activo digital a dos destinatarios, problema conocido como doble envío o gasto.

DLT-BC o Blockchain consiste en un registro de datos distribuido y descentralizado el cual preserva la totalidad de las transacciones sobre activos digitales que son efectuadas por un conjunto de individuos. Las transacciones se agrupan en un contenedor denominado bloque [39]. Este nuevo bloque es sometido a validación por los miembros de la red, llamados nodos mineros, quienes aplican el algoritmo de consenso definido en la Blockchain, y una vez es validado y aprobado, se encadena el nuevo bloque aplicando una función Hash que toma información de los bloques precedentes. Después de que un bloque es adicionado a la Blockchain, no podrá

ser eliminado o modificado sin la colusión de la mayoría, puesto que una alteración de la cadena implica rehacer todos los identificadores Hash involucrados en la producción de los bloques.

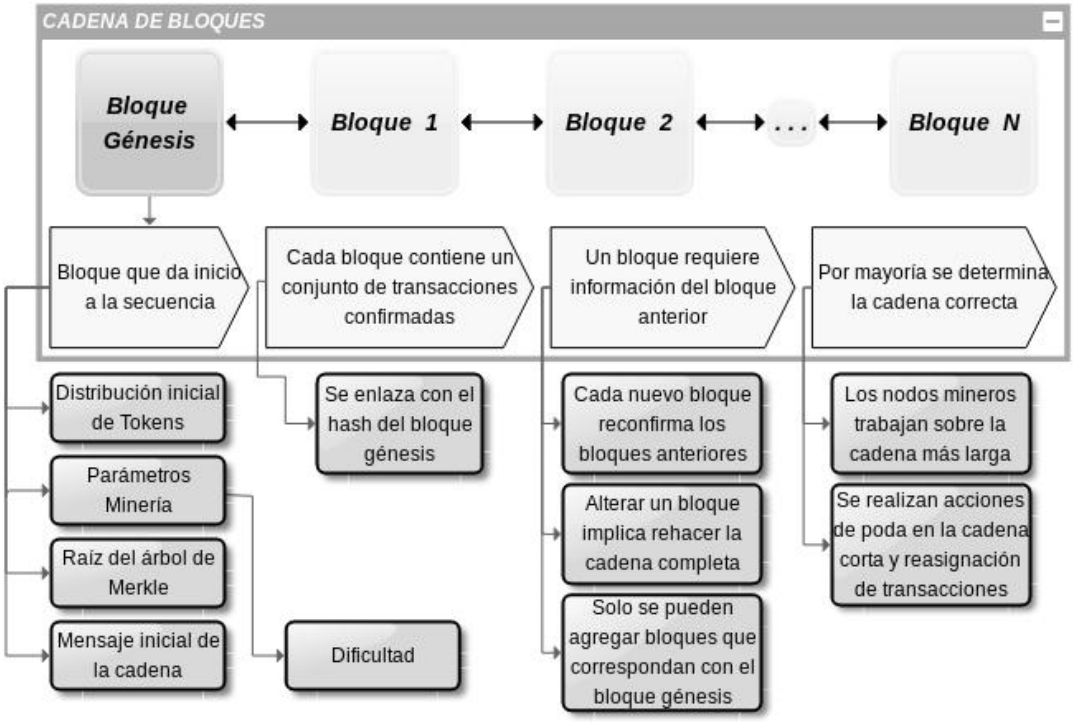

Figura 1. Proceso de inicialización y construcción de una Blockchain - DLT-BC - Fuente: Autor.

El primer bloque es denominado “Bloque Génesis", no contiene Hash de bloque predecesor, define los parámetros iniciales para el proceso de minería, realiza la primera emisión de los tokens, además de definir la información necesaria para el enlace de nodos mineros a la Blockchain, este proceso se ilustra en la Figura 1.

a. Características de DTL-BC

La implementación de un DLT-BC tiene en cuenta las siguientes características [18]:

Privacidad: El modelo propuesto en bitcoin modifica el esquema de privacidad centralizado, el cual requiere un tercero que se asume de confianza y tiene la responsabilidad de gestionar las credenciales de identificación y las transacciones de todos los actores del proceso, por lo cual limita el acceso a la información y decide cuáles datos pueden ser publicados; y lo sustituye con un registro público e inmutable de las operaciones, con la ventaja de disponer de privacidad para los usuarios al permitir un anonimato mediante el uso de llaves públicas y privadas; puesto que una transacción se firma mediante la llave privada y se verifica mediante la llave pública (ver Figura 2). Es factible asociar una identidad real con una llave pública mediante la correlación del uso de la llave pública con información personal disponible en los sitios web donde se realizó la transacción, este proceso de desanonimizar la identidad deja a los usuarios en escenarios de pseudo-privacidad [7].

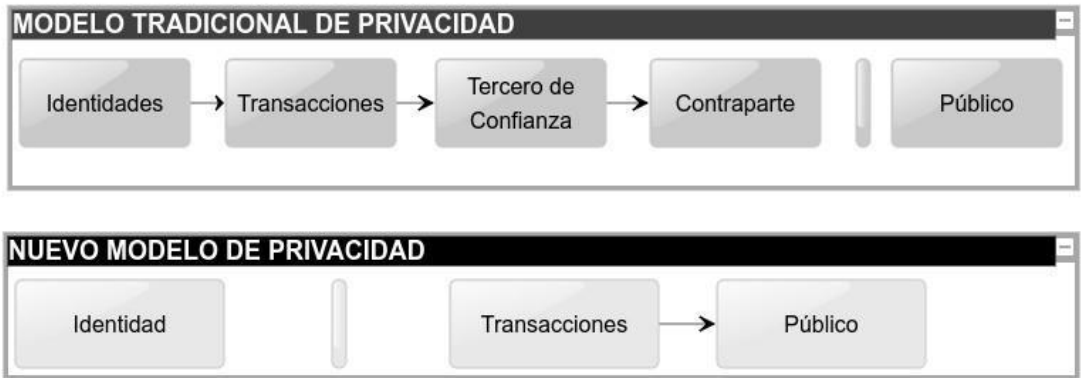

Figura 2. Modelo de privacidad actual vs Modelo de privacidad por Nakamoto. Fuente: [36]

Este modelo de privacidad requiere de la implementación de nuevos esquemas de identidad centrados en el usuario, que le permita a estos retomar el control de su información personal y la autogestión de permisos de consulta sobre la misma, es decir, esquemas de identidad descentralizada y autogobernada [3]. Además, se requieren políticas de intermediación estatal que no atenten contra la privacidad de los usuarios y su derecho al anonimato, pero sin generar espacios que permitan un actuar inapropiado de individuos.

Escalabilidad: DLT-BC opera bajo una red distribuida y descentralizada, los nodos se pueden adicionar sin restricciones en Blockchain públicas o con autorización en esquemas privados o federados. Este diseño facilita la escalabilidad horizontal de la red, pero se debe ajustar de forma automática la dificultad de generación de un bloque para mantener el tiempo de generación de bloques cercano al valor definido en el diseño del DLT-BC.

Este tiempo entre bloques es importante para permitir una correcta difusión de los nuevos bloques adicionados a la cadena. Por otro lado, este tiempo entre bloques unido al tamaño limitado y fijo de cada uno de ellos limita la concurrencia del sistema. El bloque es un contenedor de transacciones, su tamaño predefinido determina la cantidad de transacciones que puede almacenar, y la integridad de la información depende de la difusión de los nuevos bloques entre todos los nodos participantes, es por esto que el protocolo de una Blockchain fija el tiempo mínimo que debe existir entre dos bloques consecutivos. En la Figura 3 se puede visualizar el desempeño de la Blockchain de bitcoin. Se definió un tamaño de bloque de un 1 Mb, con un tamaño promedio en su ejecución de 1.28 Mb, un promedio de 1956 transacciones por bloque, con un máximo histórico de 2734 transacciones. El tiempo teórico entre bloques es de 10 minutos y se presenta un tiempo promedio de confirmación de 7.4 minutos, con valores máximos cercanos a los 30 minutos. La Blockchain está diseñada con una concurrencia de máximo 7 transacciones por segundo (TPS) y en la práctica se observa un promedio de 3.1 TPS [19].

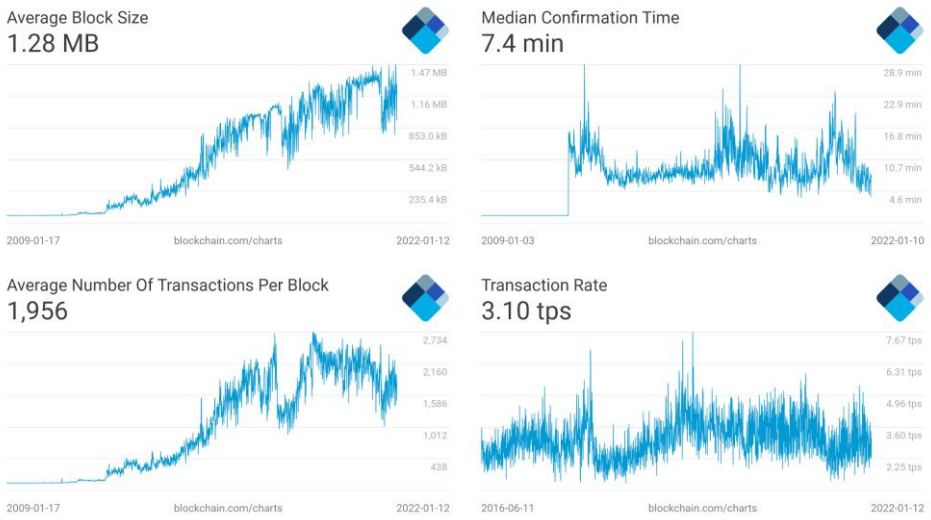

Figura 3. Gráficos desempeño de la Blockchain de bitcoin Fuente: [40]

Gobernanza: La migración de un entorno centralizado donde se permite un control y presión directa sobre el sistema, facilitando su regulación, restricción y manipulación, hacia un ecosistema descentralizado y autorregulado demanda la actualización de las políticas de gestión al interior de las organizaciones, y la adaptación de marcos metodológicos de gestión corporativa, que permita el flujo de información centrado en los usuarios y la toma de decisiones avaladas por la comunidad que integre el ecosistema Blockchain. Por otro lado, el diseño de la Blockchain debe definir el nivel de descentralización que desee, desde un entorno público, totalmente descentralizado hasta un esquema federado en el cual se dispone de un grupo de nodos que gobiernan la red [8].

Sistema de consenso: Un DLT-BC implementa un algoritmo de consenso (Blockchain consensus algorithm) orientado a preservar la integridad de la información. El consenso establece mecanismos para la gobernanza descentralizada de la red, la estructura del quórum, la autentificación, la integridad, el no repudio de transacciones, la tolerancia a fallas y la concurrencia de la Blockchain. Por otro lado, el método de consenso permite a los nodos mineros de la red comprobar las transacciones, y conservar un historial único de transacciones. Finalmente, un intento de adulteración requiere rehacer la firma de cada uno de los bloques escritos en la cadena, hasta el bloque génesis [20]. Por ejemplo, en bitcoin se implementó como algoritmo de consenso una prueba de trabajo (Proof of Work - PoW), la cual requiere encontrar un Hash para el nuevo bloque con una determinada cantidad de ceros al inicio, este cálculo demanda grandes recursos computacionales.

El algoritmo de prueba de trabajo requiere de nodos denominados mineros, los cuales deben disponer de hardware dedicado, preferiblemente diseñado para calcular la función Hash que implemente la Blockchain, y compiten por encontrar el Hash del siguiente bloque para agregarlo a la cadena y obtener los tokens de remuneración respectivos. El algoritmo de consenso define la política de incentivos que estimulará un

comportamiento benigno de los actores, reduciendo el riesgo de colusión de sus participantes. Por último, una Blockchain tipo bitcoin es tolerante a fallos bizantinos, y requiere por lo menos que 2 tercios de los participantes permanezcan honestos para preservar la integridad del registro, con la limitación que un nodo no conoce con exactitud el instante en que el consenso es alcanzado en la red, y asume con alguna probabilidad que este se logra en el tiempo, razón por la cual se requiere un proceso en tiempo constante para agregar los nuevos bloques en la cadena, posibilitando que el conjunto de nodos mineros pueda decidir y validar sobre la cadena más larga.

Fortalezas:

- Implementa un registro distribuido de información, que es almacenado en los nodos mineros, y permite a los miembros de la red un acceso a los datos con alta disponibilidad y tolerancia a fallos.
- No requiere de un tercero de confianza para garantizar la integridad de la información, ya que la tecnología proporciona confianza entre las partes por medio de firmas digitales y un servidor de marcas de tiempo.
- La no implementación de una autoridad central permite al sistema ser resistente a manipulación y censura.
- La red es escalable horizontalmente permitiendo la adición o remoción de nodos de forma transparente.
- El historial de transacciones es público por lo que cualquier usuario puede consultarlo y participar si dispone de los recursos como nodo minero.
- Es tolerante a fallas bizantinas [6] y sus datos son inmutables en el tiempo.
- Dispone de un mecanismo para la automatización de reglas de negocio denominado contratos inteligentes [28].

Amenazas:

- La necesidad de empaquetar las transacciones en un contenedor, denominado bloque, limita por diseño el número de transacciones concurrentes en un DLT-BC. Además, el tiempo de creación y difusión de un bloque ralentiza la confirmación de transacciones en comparación con un sistema de validación de pagos centralizado como la red VISA [9].
- El algoritmo de consenso es ambientalmente cuestionable en los sistemas que utilizan prueba de trabajo, puesto que a medida que aumenta la cantidad de nodos mineros, se incrementa de forma automática la dificultad para la generación de un bloque, con el objeto de mantener estable el tiempo entre estos, situación que produce aumento en el consumo de energía debido al incremento en el procesamiento computacional. Por ejemplo, una transacción de bitcoin puede requerir alrededor de 200 kw/h, 37 kw/h en Ethereum y 0.01 Kw/h en VISA [9],[41].

- El éxito de un nodo minero depende de la efectividad de su hardware para calcular la función Hash que use la Blockchain, por lo cual se hace necesario disponer de hardware dedicado; y a medida que varía la dificultad es necesario el uso de Application Specific Integrated Circuits - ASIC -. Los cálculos realizados para encontrar el Hash del bloque n no se pueden utilizar para el bloque n+1, generando un significativo consumo no aprovechable de energía eléctrica.
- Un nodo completo o minero debe disponer de una copia completa de la Blockchain, lo que demanda mayor espacio de disco a medida que la Blockchain aumenta sus transacciones en el tiempo. La Blockchain de bitcoin requiere 385 GB de almacenamiento [40].
- El modelo de pseudo privacidad propuesto por Nakamoto que publica el total de transacciones de los participantes en un entorno inmutable genera riesgos a la privacidad y reputación de los usuarios en caso de ser divulgada la información de un propietario de una clave pública [21].

b. Tecnología de registro distribuido basado en DAG - DLT-DAG

La aplicación de grafos dirigidos acíclicos -DAG- está dinamizando la evolución de los DLT, dadas las características que mejoran aspectos fundamentales de Blockchain relacionados con la concurrencia, escalabilidad, costos de transacciones y métodos de consenso [30]. Un DLT con una estructura de datos basada en un grafo acíclico dirigido -DAG- enlaza directamente las transacciones sin la necesidad de agruparlas en un bloque, con una funcionalidad similar a una Blockchain en la preservación y distribución de un registro inmutable de eventos con un ordenamiento topológico. DLT-DAG se despliega sobre un conjunto de nodos configurados en una red peer-to-peer, donde cada nodo dispone de una copia local del DAG, que se actualiza mediante un intercambio de mensajes (algoritmo gossip) entre sus vecinos [30]. La validación de una transacción se basa en información de confirmación de transacciones previas, por lo cual no es necesario un proceso de minería, lo que reduce el costo de una transacción, hasta inclusive hacerlo inexistente [31]. Por ejemplo, la DLT Hashgraph tiene un tiempo teórico de confirmación de transacción entre 3 y 5 segundos, con un promedio real de 2.96 segundos, con 26000 TPS de concurrencia teórica y 10000 TPS logrados en la práctica [42].

Por otro lado, la adopción de esta tecnología disruptiva debe incluir el análisis de interoperabilidad, el diseño de control de cambios o migración para los sistemas informáticos actuales y un reporte de los beneficios/retos en su adopción. En el caso de DLT se requiere la definición de metodologías para el diseño y arquitectura de los sistemas de información que integre el modelado de la organización (EM), el diseño de arquitectura empresarial (EA) y el gobierno corporativo de TI (EGIT), por ejemplo, en [32] se propone un *Framework* para tecnologías Blockchain (DLT-BC) centrado en escenarios de aplicación y casos de uso.

c. Comparación DLT-BC y DLT-DAG

La Figura 4 presenta una comparación de la tecnología de registro distribuido dividida en sus dos categorías: (1) con bloque - DLT-BC, parte izquierda de la figura y (2) sin bloque - DLT-DAG, a la derecha.

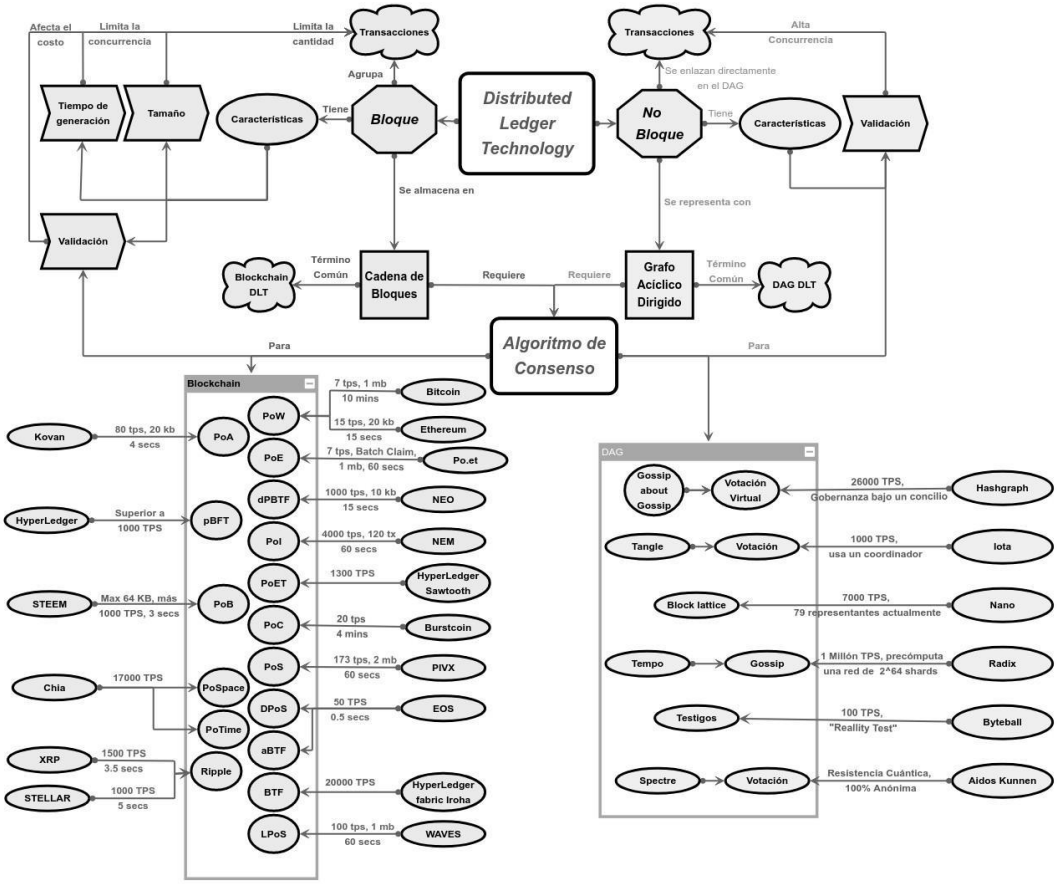

Figura 4. Características de DLT-BC vs DLT-DAG Fuente: Autor

DLT-BC presenta el bloque como unidad de estructura, los cuales serán enlazados en una lista encadenada, cada bloque tiene un tamaño fijo, que acota el número de transacciones que puede contener y un tiempo de generación entre bloques que debe permanecer aproximadamente constante para garantizar la correcta difusión de la cadena más larga.

El tamaño del bloque y el tiempo de creación entre estos afecta la cantidad de transacciones por segundo e incrementa el costo de validación de estas; por otro lado, DLT-DAG enlaza directamente las transacciones entre sí por medio de un grafo acíclico dirigido, las nuevas transacciones pueden ser confirmadas a partir de las transacciones previas, lo que permite una alta concurrencia en el sistema. Los dos modelos aplican un algoritmo de consenso para preservar la integridad de la información; en DLT-BC se tiene una variedad conceptual en los enfoques de los algoritmos de consenso, por ejemplo, el algoritmo de prueba de trabajo implementado por

bitcoin, que se basa en un problema NP-completo, presenta una concurrencia máxima de 7 TPS, con un tamaño de bloque de 1 mb y un tiempo de generación de 10 minutos, o 15 TPS, mientras que en DLT-DAG el algoritmo de consenso se basa principalmente en la definición de mecanismos de difusión de mensajes para actualizar la información local de los nodos participantes con el objeto de sincronizar la información de las transacciones.

d. Escenarios de aplicación de DLT

La aplicación de DLT tiene como ámbito los procesos donde se requiera un registro inmutable, confiable y visible sobre un flujo de información, razón por la cual en los últimos años se ha notado un crecimiento de soluciones informáticas soportadas en DLT, y que abarcan diversos sectores como: salud, educación, economía, cadena de suministro, IoT y gobierno [4],[45].

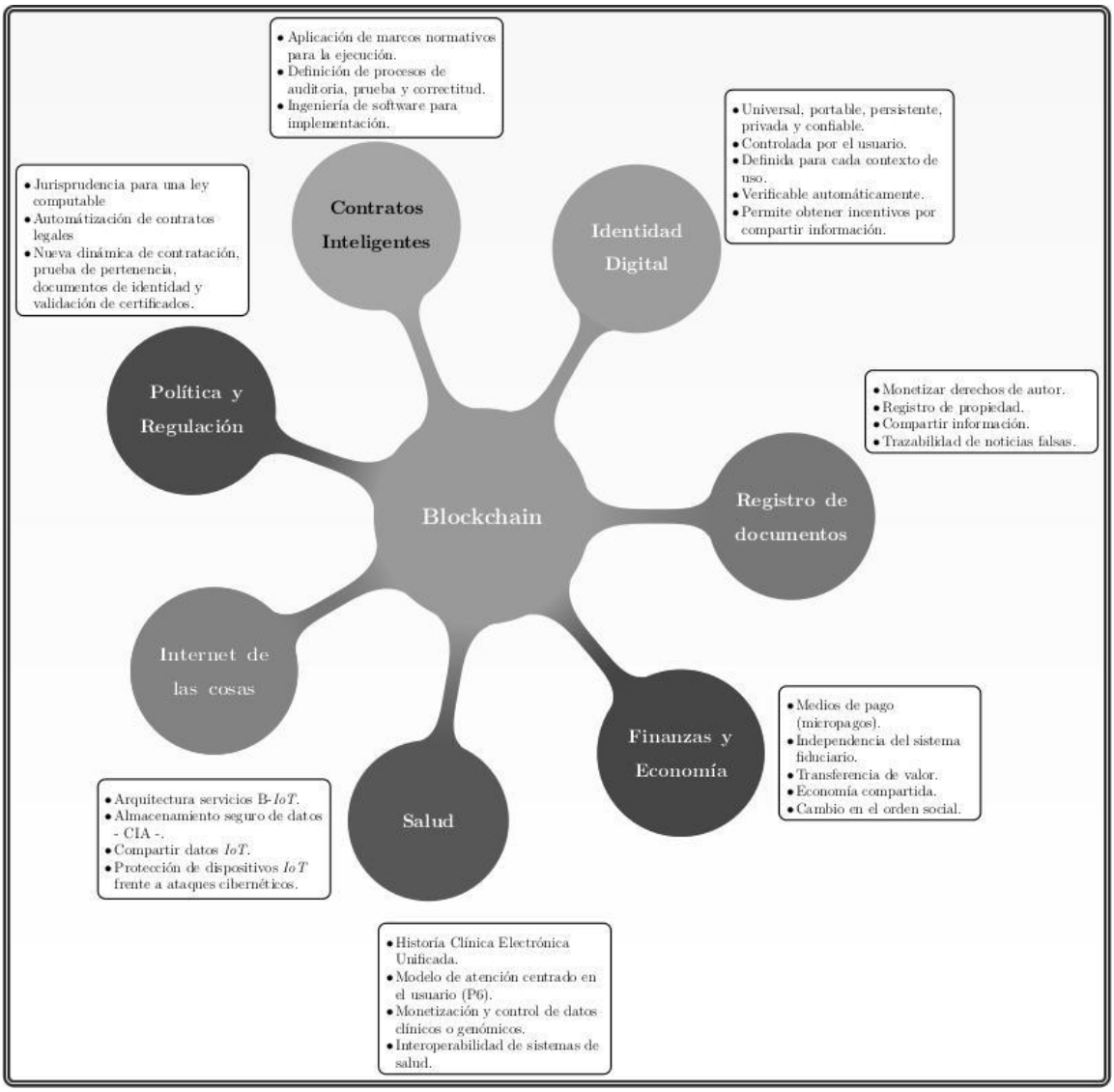

Figura 5. Áreas generales de aplicación de la tecnología de registro distribuido -DLT-. Fuente: Autor

En la Figura 5 se presentan los escenarios de aplicación de la tecnología de registro distribuido, enumerando los puntos concretos de uso en cada caso.

En primer lugar, en el sector económico, específicamente en lo relacionado a medios de pago y transferencia de valor, es visible un mayor impacto de esta tecnología orientado principalmente desde el desarrollo de las criptomonedas descentralizadas, sector de influencia más representativo, y factor dinamizador de los procesos en investigación, regulación e innovación sobre DLT. Para el mes de enero del año 2022 se reportan en Coinmarketcap 16762 criptomonedas, que son aceptadas como medio de pago o para intercambio entre estas, con una capitalización de mercado de $2,040,088,944,284 USD y un movimiento diario superior a los $ 100 billones USD, y una dominación del bitcoin respecto al valor total de transacciones, superior al 39.9 % [43].

La influencia de DLT en los mercados de valores se ha debido principalmente a dos razones: (I) la aplicación pionera de DLT-Blockchain fue la criptomoneda bitcoin, y durante los primeros años de desarrollo los conceptos de Blockchain y bitcoin estuvieron fuertemente entrelazados.; y (II) la evolución de DLT ha estado estrechamente relacionada con la creación de criptomonedas, puesto que estas han sido un mecanismo exitoso para captar fondos (crowdfunding) con el objeto de financiar proyectos de aplicación específicos.

En segundo lugar, en el cuidado de la salud la tecnología DLT se ha perfilado como el soporte tecnológico necesario para la implementación del modelo de atención en salud P6, facilitando la interoperabilidad entre los actores del sector salud, garantizando la privacidad de la información y posibilitando al usuario el control de su historia clínica [22]. Por lo tanto DLT permitirá el diseño de un escenario seguro, confiable, trazable y ubicuo para compartir información clínica, lo que facilitará procesos de investigación médica para un diagnóstico oportuno y personalizado del paciente, agregando una capa de seguridad que administrará eficientemente los dispositivos médicos IoT (MIoT) para el monitoreo del estado de salud del paciente.

Por otro lado, este entorno de flujo de información provee las condiciones necesarias y suficientes para la atención integral en salud que facultará una medicina predictiva con la capacidad de estimar ocurrencias posibles de enfermedades por la proyección de estados futuros de salud del paciente, logrando una medicina preventiva y personalizada, dotada de herramientas para diagnóstico temprano con tratamientos personalizados que mejoran el desempeño del mismo y reducen los efectos secundarios. La industria de la salud debe prepararse para un cambio que tiende a una medicina con datos públicos previo consentimiento de los involucrados, que permita la colaboración de las comunidades en entornos confidenciales, con una participación del paciente en su proceso de enfermedad [23],[24],[26]. En esta área se han desarrollado aplicaciones para trazabilidad en la cadena de suministro [25], registros médicos, interoperabilidad [27].

En tercer lugar, la Internet de las cosas dispondrá con DLT de una capa de seguridad que permitirá verificar y autorizar los dispositivos IoT con el objeto de mantener la información confiable [10],[11]. En cuarto lugar,

respecto a la aplicación de contratos inteligentes, política y regulación [29], DLT está modificando los procesos de gestión en las organizaciones, siendo necesarias nuevas prácticas para el desarrollo de plataformas tecnológicas corporativas, que permitan automatizar los procedimientos legales para efectuar pagos, agilizar el sistema de registro de bienes y servicios, democratizar el acceso a la información y, aún más importante, producir un cambio cultural que permitirá un empoderamiento de los individuos hacia el control de las instituciones como factor clave de transparencia y eficiencia; esto más que una revolución industrial basada en tecnología es una revolución social.

En quinto lugar, es un derecho fundamental del individuo la capacidad de probar, administrar y preservar su identidad física y digital, por lo cual los gobiernos deben establecer mecanismos para la identificación de los ciudadanos, además de regular el uso de datos personales, sin afectar la privacidad de las personas [45], y además, la identidad digital descentralizada debe ser creada y administrada por el usuario, permitiendo definir un subconjunto de identidades dependiendo del servicio al que se requiera acceder.

Además, la creación de una identidad digital autogobernada (SSI) donde la información personal se encuentra bajo el control del propietario de la misma [14],[15], como se propone en Sovrin [45] o uPort [47], se debe diferenciar de una identidad confiable descentralizada donde se combina el uso de credenciales confiables, como un documento de identidad generado por una organización gubernamental, como un pasaporte, con verificación bajo DLT, por ejemplo, ShoCard [48] y Civic [49]; pero en ambos escenarios se debe disponer de seguridad, control y portabilidad de la identidad.

Finalmente, el registro de propiedad basado en una entidad centralizada, por ejemplo, una dependencia de notariado y registro, puede generar problemas en la certificación y legalidad del registro de propiedad, ya que la confianza del proceso recae completamente sobre la honestidad de la entidad que los emite. Por otro lado, los derechos de propiedad intelectual se hacen difíciles de ejercer en contextos dinámicos como Internet, donde se dificulta monetizar correctamente la utilización de material registrado, por ejemplo, en las redes sociales la información fluye y se usa de manera vertiginosa, con orígenes y propietarios de difícil trazabilidad, por lo cual, un sistema para la gestión de derechos de autor implementado en una Blockchain, validado mediante contratos inteligentes permite automatizar los pagos asociados a uso de material registrado.

La Blockchain llevará un registro de generación de contenidos con la respectiva asignación de derechos de autor (Procedencia) y el control de transacciones asociadas al consumo de contenido. Por ejemplo en [33] se presenta la arquitectura de un sistema Blockchain para gestión de actas de nacimiento, [34] diseña un sistema de archivo personal descentralizado, inmutable y seguro, [35] describe un servicio de notariado para almacenar y compartir datos personales en una Blockchain privada tipo ethereum. En [16] se estudia la trazabilidad y control sobre generación de noticias falsas.

III. Observaciones finales

La Tecnología de Registro Distribuido - DLT - surgió en el año 2008 con bitcoin, que se concibió como un sistema de pagos peer-to-peer soportado en una cadena de bloques con un servidor de marcas de tiempo para verificar las transacciones, y en un periodo de tiempo de aproximadamente cinco (5) años extendió su campo de aplicación de las criptomonedas a diferentes áreas como salud, gestión de documentos, Internet de las cosas y, en general, a cualquier escenario que sea susceptible de validar y auditar un activo digital.

Por otra parte, la blockchain de bitcoin permite analizar el desempeño de este tipo de sistemas ya que se dispone de datos históricos a partir del 3 de enero de 2009, marca de tiempo de su bloque génesis [49], lo que permite el análisis del rendimiento de la blockchain, detección y predicción de los cuellos de botella y la afectación del sistema debido a la dinámica de conexión y desconexión de nodos mineros que afectan directamente la capacidad de procesamiento de Hash de la red.

Dados los inconvenientes de desempeño que se han presentado con bitcoin, unido con la aparición de nuevos casos de aplicación, se ha generado un incremento exponencial de los proyectos de aplicación de DLT, en lo cuales se han modificado dos componentes fundamentales del DLT como son: (1) la estructura de datos dividiendo la DLT en dos grupos, con bloque denominado DLT-BC o Blockchain y DLT sin bloque donde se enlazan directamente las transacciones, principalmente en grafos acíclicos dirigidos DLT-DAG; y (2) el método de consenso, con el objeto de reducir el costo de las transacciones y aumentar la concurrencia.

Finalmente, DLT generará un impacto social ya que el almacenamiento confiable y público de registros permitirá a través del tiempo un empoderamiento de los actores de un sistema, como son ciudadanos, clientes, inversores, pacientes o dispositivos IoT, el cual se reflejará en nuevos esquemas de control y vigilancia, y permitirá un uso eficiente y controlado de los recursos dentro de las organizaciones por medio de la automatización de verificación de condiciones de cumplimientos en los acuerdos de niveles de servicio contratados; por ejemplo, se pueden verificar las condiciones de transporte de almacenamiento de un medicamento y una vez que llega a su destino determinar mediante información recolectada por dispositivos IoT y almacenada en un DLT, si durante todo el proceso de la cadena de suministro el producto se ha preservado dentro de los parámetros correctos para su aceptación.

IV. Referencias

[1] P. Tasca and C. J. Tessone, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification," Ledger, vol. 4, pp. 1–39, 2019, doi: 10.5195/ledger.2019.140.

[2] G. Suciu et al., "Comparative Analysis of Distributed Ledger Technologies," 6th Glob. Wirel. Summit, GWS 2018, pp. 370–373, Nov. 2019, doi: 10.1109/GWS.2018.8686563.

[3] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, “A survey on essential components of a self-sovereign identity,” Comput. Sci. Rev., vol. 30, pp. 80–86, 2018, doi: 10.1016/j.cosrev.2018.10.002.

[4] Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. International Journal of Information Management, 49 (February), 114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005

[5] R. A. DeMillo, Foundations of Secure Computation. Orlando, FL, USA: Academic Press, Inc., 1978. ISBN 0122103505.

[6] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem,” ACM Trans. Program. Lang. Syst., vol. 4, no. 3, pp. 382–401, 1982, doi: 10.1145/357172.357176.

[7] J. Bernal Bernabe, J. L. Canovas Sanchez, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, “Privacy-Preserving Solutions for Blockchain: Review and Challenges,” IEEE Access, vol. 7, no. November, pp. 164908–164940, 2019, doi: https://doi.org/10.1109/ACCESS.2019.2950872.

[8] M. Herlihy, “Blockchains from a distributed computing perspective,” Commun. ACM, vol. 62, no. 2, pp. 78–85, 2019, doi: 10.1145/3209623.

[9] J. Truby, “Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies,” Energy Res. Soc. Sci., vol. 44, no. February, pp. 399–410, 2018, doi: 10.1016/j.erss.2018.06.009.

[10] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang, “Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends,” IEEE Trans. Syst. Man, Cybern. Syst., vol. 49, no. 11, pp. 1–12, 2019, doi: 10.1109/TSMC.2019.2895123.

[11] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, “Blockchain’s adoption in IoT: The challenges, and a way forward,” J. Netw. Comput. Appl., vol. 125, no. March 2018, pp. 251–279, 2019, doi: 10.1016/j.jnca.2018.10.019.

[12] P. Schueffel, “Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph - A High-Level Overview and Comparison,” Soc. Sci. Res. Netw. - SSRN, vol. December, pp. 1–8, 2018, doi: 10.2139/ssrn.3144241.

[13] L. Hughes, Y. K. Dwivedi, S. K. Misra, N. P. Rana, V. Raghavan, and V. Akella, “Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda,” Int. J. Inf. Manage., vol. 49, no. February, pp. 114–129, 2019, doi: 10.1016/j.ijinfomgt.2019.02.005.

[14] G. Goodell and T. Aste, “A Decentralized Digital Identity Architecture,” Front. Blockchain, vol. 2, no. November, pp. 1–19, 2019, doi: 10.3389/fbloc.2019.00017.

[15] P. Dunphy and F. A. P. P. Petitcolas, “A first look at identity management schemes on the blockchain,” IEEE Secur. Priv., vol. 16, no. 4, pp. 20–29, 2018, doi: 10.1109/MSP.2018.3111247.

[16] P. Fraga-Lamas and T. M. Fernández-Caramés, “Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality,” *IT Prof.*, vol. 22, no. 2, pp. 53–59, 2020, [Online]. Available: https://ieeexplore.ieee.org/document/9049288.

[17] X. Xu et al., “A taxonomy of blockchain-based systems for architecture design,” in 2017 IEEE International Conference on Software Architecture (ICSA), 2017, pp. 243–252, doi: 10.1109/ICSA.2017.33.

[18] W. Li, A. Sforzin, S. Fedorov, and G. O. Karame, “Towards Scalable and Private Industrial Blockchains,” in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts - BCC ’17, 2017, pp. 9–14, doi: 10.1145/3055518.3055531.

[19] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the Security and Performance of Proof of Work Blockchains,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS’16, 2016, pp. 3–16, doi: https://dl.acm.org/doi/10.1145/2976749.2978341.

[20] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications,” in 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017, pp. 1–5, doi: https://doi.org/10.1109/ICACCS.2017.8014672.

[21] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. 2014. Deanonymisation of Clients in Bitcoin P2P Network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). Association for Computing Machinery, New York, NY, USA, 15–29. DOI:https://doi.org/10.1145/2660267.2660379

[22] R. Pava, J. N. Perez Castillo, y L. F. Niño Vasquez, «Perspectiva para el uso del modelo P6 de atención en salud bajo un escenario soportado en IoT y blockchain», Tecnura, vol. 25, n.º 67, pp. 112–130, enero. 2021.

[23] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” J. Netw. Comput. Appl., vol. 135, no. January, pp. 62–75, 2019, doi: 10.1016/j.jnca.2019.02.027.

[24] S. G. Alonso, J. Arambarri, M. López-Coronado, and I. de la Torre Díez, “Proposing New Blockchain Challenges in eHealth,” J. Med. Syst., vol. 43, no. 3, p. 64, 2019, doi: 10.1007/s10916-019-1195-7.

[25] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, “Blockchains everywhere - a use-case of blockchains in the pharma supply-chain,” in 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, pp. 772–777, doi: 10.23919/INM.2017.7987376.

[26] M. Hölbl, M. Kompara, A. Kamišali, and L. Nemec, “A Systematic Review of the Use of Blockchain in Healthcare,” Symmetry (Basel)., vol. 10, no. 470, pp. 1–22, 2018, doi: https://doi.org/10.3390/sym10100470.

[27] C. Agbo, Q. Mahmoud, and J. Eklund, “Blockchain Technology in Healthcare: A Systematic Review,” Healthcare, vol. 7, no. 2, p. 56, 2019, doi: 10.3390/healthcare7020056.

[28] B. K. Mohanta, S. S. Panda, and D. Jena, “An Overview of Smart Contract and Use Cases in Blockchain Technology,” in 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1–4, doi: 10.1109/ICCCNT.2018.8494045.

[29] D. S. Pradeepkumar, K. Singi, V. Kaulgud, and S. Podder, “Evaluating complexity and digitizability of regulations and contracts for a blockchain application design,” in 2018 ACM/IEEE 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, May 2018, no. 1, pp. 25–29, doi: 10.1145/3194113.3194117.

[30] H. Pervez et al., “A Comparative Analysis of DAG-Based Blockchain Architectures,” ICOSST 2018 - 2018 Int. Conf. Open Source Syst. Technol. Proc., no. March, pp. 27–34, 2019, doi: 10.1109/ICOSST.2018.8632193.

[31] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, “Inclusive Block Chain Protocols with bitcoin details,” in International Conference on Financial Cryptography and Data Security, 2015, pp. 528–547, doi: 10.1007/978-3-662-47854-7_33.

[32] H. C. Lim, “Enterprises and Future Disruptive Technological Innovations: Exploring Blockchain Ledger Description Framework (BLDF) for the Design and Development of Blockchain Use Case,” in Advances in Information and Communication, 2020, vol. 70, pp. 533–540, doi: 10.1007/978-3-030-12385-7_39.

[33] N. Buchmann, C. Rathgeb, H. Baier, C. Busch, and M. Margraf, “Enhancing Breeder Document Long-Term Security Using Blockchain Technology,” in Proceedings - International Computer Software and Applications Conference, 2017, vol. 2, pp. 744–748, doi: 10.1109/COMPSAC.2017.119.

[34] Z. Chen and Y. Zhu, “Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging,” Proc. - 2017 IEEE 6th Int. Conf. AI Mob. Serv. AIMS 2017, pp. 93–99, 2017, doi: 10.1109/AIMS.2017.31.

[35] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, “Blockchain as a Notarization Service for Data Sharing with Personal Data Store,” in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data

Science And Engineering (TrustCom/BigDataSE), 2018, pp. 1330–1335, doi: 10.1109/TrustCom/BigDataSE.2018.00183.

[36] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008. Consultado en Diciembre 20 de 2021, disponible en: https://bitcoin.org/en/

[37] C. Dwork and M. Naor, “Pricing via Processing or Combatting Junk Mail,” in Advances in Cryptology --- CRYPTO’ 92, 1993, pp. 139–147, Consultado en Noviembre 17 de 2021, disponible en: https://web.cs.dal.ca/~abrodsky/7301/readings/DwNa93.pdf.

[38] H. Massias and X. S. A. J.-J. Quisquater, “Desing of a secure timestamping service with minimal trust requeriment” 1999. Consultado en Septiembre 1 de 2021, disponible en: https://nakamotoinstitute.org/static/docs/secure-timestamping-service.pdf

[39] M. Swan, Blockchain: Blueprint for a New Age, vol. 1. O’Reilly Media, Inc., 2015.

[40] Blockchain luxemburg S.A, “Blockchain Charts. The most trusted source for data on the bitcoin blockchain” 2021. Consultado en Enero 13 de 2022, disponible en: https://www.blockchain.com/charts

[41] F. Analysis et al., “Why Bitcoin transactions are more expensive than you think,” ING Groep N.V., 2017. Consultado en Noviembre 3 de 2021, disponible en: https://think.ing.com/opinions/why-bitcoin-transactions-are-more-expensive-than-you-think/

[42] Cryptocurrency Market Capitalizations - CoinMarketCap 2020. Consultado en Enero 13 de 2022, disponible en: https://coinmarketcap.com/

[43] Nomura Research Institute. (Marzo 2016). Survey on Blockchain Technologies and Related Services, [en línea]. Consultado en Octubre 31 de 2021, disponible en: https://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf

[44] T. Lyons, L. Courcelas, and K. Timsit, “Blockchain and digital identity,” 2019. Consultado en Agosto 7 de 2021, disponible en: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

[45] D. R. Phil Windley, “Sovrin : A Protocol and Token for Self-Sovereign Identity and Decentralized Trust A White Paper from the Sovrin Foundation,” Sovrin.Org, 2018. Consultado en Junio 23 de 2020, disponible en: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[46] ConsenSys AG’s uPort, “uPort - Tools for Decentralized Identity and Trusted Data” 2020. Consultado en Octubre 17 de 2021, disponible en: https://www.uport.me/

[47] ShoCard Inc, “Identity management verified using the blockchain,” 2017. Consultado en Agosto 27 de 2021, disponible en: https://shocard.com/wp-content/uploads/2019/02/ShoCard-Whitepaper-2019.pdf

[48] Civic Technologies, “Civic whitepaper” 2017. Consultado en Mayo 15 de 2021, disponible en: https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf

[49] Blockchain.com, “Block 0 - Bitcoin explorer” 2021. Consultado en Diciembre 16 de 2021, disponible en: https://www.blockchain.com/btc/block/0

Publicación Facultad de Ingeniería y Red de Investigaciones de Tecnología Avanzada – RITA

REVISTA

TIA