

Recibido: 4 de febrero 2026 / Aceptado: 18 de mayo 2026

GESTIÓN DOCUMENTAL DE ACTIVOS DIGITALES CON HYPERLEDGER FABRIC E IPFS CLUSTER

DIGITAL ASSET RECORDS MANAGEMENT USING HYPERLEDGER FABRIC AND IPFS CLUSTER

Roger Calderón Moreno¹, Carlos Danilo Núñez Gil² Edgar David Lozada González³

Resumen:

Se propuso construir un prototipo de un componente de software soportado sobre blockchain y un sistema almacenamiento distribuido, que apoye la preservación a largo plazo de los documentos electrónicos. Para la preservación digital se definió utilizar a Hyperledger Fabric una blockchain de tipo permissionado y al IPFS, apoyados en un software como servicio que permitiera gestionar Activos Digitales, software que fue evaluado para dos escenarios de prueba. Se evidenció que las transacciones sobre entornos de blockchain de tipo público son costosas computacionalmente por sus mecanismos de validación de transacciones, con Hyperledger Fabric se observa que los tiempos son bajos y se mantienen constantes ante el aumento de bloques en la cadena. Dicha situación se puede explicar por el mecanismo de consenso que no requiere que todos los nodos validen las transacciones, ya que el principio fundamental es la confianza entre las partes.

Palabras claves: Gestión documental, Blockchain, Hyperledger, IPFS, Activo Digital, Cluster.

Abstract

It was proposed to build a prototype of a software component supported on blockchain and a distributed storage system, which supports the

long-term preservation of electronic documents. For digital preservation, Hyperledger Fabric was defined as a blockchain of permitted type and IPFS, supported by a software as a service that allowed the management of Digital Assets, software that was evaluated for two test scenarios. It is evident that transactions on public blockchain environments are computationally expensive due to their transaction validation mechanisms. With Hyperledger Fabric it is observed that the times are low and remain constant with the increase in blocks in the chain. This situation can be explained by the consensus mechanism that does not require all nodes to validate the transactions, since the fundamental principle is trust between the parties.

Keywords: Document management, Blockchain, Hyperledger, IPFS, Digital Asset., Cluster.

1. Introducción

En Colombia las entidades públicas tienen el deber de implementar las políticas de gestión documental dadas por el Archivo General de la Nación Jorge Palacios Preciado (AGN), en relación a los documentos electrónicos se deben preservar a largo plazo atendiendo al Artículo N.13 de la Ley 594 de 2000 [1] que dice: Los documentos electrónicos podrán conservarse, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure su originalidad, así como la autenticidad, la integridad, la disponibilidad y confiabilidad necesaria para

1 Magister en Software Libre, Universidad Autónoma de Bucaramanga, Colombia, Bucaramanga. Afiliación institucional: Universidad de los Llanos, Colombia. e-mail: rcalderonmoreno@unillanos.edu.co. ORCID: <https://orcid.org/0000-0001-5923-8601>

2 Ingeniero de Sistemas, Universidad de los Llanos, Colombia, Villavicencio. e-mail: carlos.nunez@unillanos.edu.co. ORCID: <https://orcid.org/0009-0002-9386-0159>

3 Ingeniero de Sistemas, Universidad de los Llanos, Colombia, Villavicencio. e-mail: edgar.lozada@unillanos.edu.co. ORCID: <https://orcid.org/0009-0004-1801-0298>

reproducirlo. Con los documentos electrónicos se ha observado que no es posible verificar fácilmente si los documentos son originales, si los documentos han sufrido modificaciones, si los metadatos han sido modificados, en ocasiones no es posible la trazabilidad de los cambios realizados. En [2] se evidenció que en Colombia el ciberdelito ha sido la tipología criminal que más ha crecido en los últimos tres años, donde se destacan: Violación de Datos Personales y el Acceso Abusivo a Sistemas Informáticos. Otro riesgo que se tiene con el procesamiento de documentos electrónicos centralizados es la exposición de la información a la posibilidad de secuestro de información a través de malware de tipo ransomware en Colombia se han presentado situaciones de este tipo como se evidencia en [3, 4, 5, 6]. El Estado colombiano ha estado motivando y orientando a las entidades del orden nacional para implementar procesos de transformación digital, invitándoles a incorporar tecnologías emergentes asociados a la Cuarta Revolución Industrial que faciliten la prestación de servicios del Estado. Dentro de las tecnologías recomendadas están los DLT (Distributed Ledger Technology), y adicionalmente la adopción de Blockchain (cadenas de bloques) [12,13].

Los procesos de Gestión Documental apoyados por las nuevas tecnologías han presentado avances, en [14,15], se indicó que la tecnología Blockchain posee un potencial enorme para su aplicación en diversas áreas de conocimiento, pero en el área de la preservación de archivos digitales no se han presentado avances significativos y que sus logros son escasos en relación a otras temáticas. La apropiación de Blockchain en la Gestión Documental ha ido avanzando lentamente. Por ejemplo, en [16] indica que el uso de Blockchain “va a solucionar un amplio problema en la industria que es el de transmitir y archivar documentos críticos y exactos”. Para [17], la gestión documental, tendrá que adaptarse y evolucionar según se va avanzando en el proceso de transformación digital, ya que está pasando de los documentos en papel a documentos electrónicos, y manifiesta que la tecnología Blockchain y los Smart Contracts cambiará drásticamente la forma de gestión documental, incluso sugiere que podría ser un sustituto de la autoridad archivística. Blockchain es definido por [18] como una tecnología que permite a las partes que no tienen una confianza particular entre sí para intercambiar cualquier tipo de datos digitales de igual a igual sin intermediario. Los datos pueden representar objetos tangibles o intangibles que puedan traducirse a un formato digital. En [27] y [28], indican que existen varios modelos para almacenar datos asociados a la Blockchain, alternativas como almacenar la información completa de los archivos dentro de la cadena de bloques, una alternativa costosa computacionalmente y en recursos económicos, así que sugieren solo almacenar los metadatos, otra alternativa es almacenar fuera de la cadena los archivos, y para ello se dispone de sistemas de archivos distribuidos, donde propusieron almacenar los datos grandes (archivos binarios) fuera de la cadena de bloques, dejando solo los metadatos más importante en la cadena junto con el hash de los archivos; hash que será necesario para el proceso de validar la integridad, autenticidad y la disponibilidad de los archivos digitales.

Por lo anterior, apoyándose en las tecnologías emergentes se propuso tratar los documentos electrónicos como Activos Digitales, los cuales se definen como un recurso digital (Digital Asset) que tiene asociado una metadata o estructura de atributos, y que representa un valor según el propietario o quien lo quiera utilizar o poseer. Se les llama activos porque se dedica un esfuerzo de tiempo y dedicación para su creación y su administración [32,33,34]. Para gestionar y procesar los Activos Digitales se planteó la necesidad construir un prototipo de un componente de software como servicio soportado sobre Blockchain y un sistema almacenamiento distribuido, que apoye la adopción de nuevas tecnologías en el proceso de preservación a largo plazo de los documentos electrónicos. A partir de las recomendaciones de los trabajos de: [36, 37, 38 y 39], se propuso que la Blockchain se soportará sobre Hyperledger Fabric y por el sistema de archivos distribuido: Inter Planetary Filing System (IPFS).

En el desarrollo de la investigación se utilizó un enfoque de investigación aplicada, ya que se adapta a la naturaleza del proyecto y de los objetivos planteados, permitiendo entregar una solución tecnológica a la sociedad académica. El prototipo de software construido permitió el almacenamiento y gestión de activos digitales, soportados con la implementación de contratos inteligentes, que en el ámbito de Hyperledger Fabric se denominan Chaincodes. Para el proyecto se definieron dos tipos de activos digitales con metadata: documentos digitales y registros de notas académicas. Adicionalmente, los documentos digitales fueron almacenados dentro de un cluster de IPFS, y en la Blockchain se almacenó el hash de cada documento junto con la metadata.

Dentro del proceso de construcción de software se utilizó una metodología de desarrollo Ágil, denominada Agile Unified Process (AUP) [42], y sobre la cual, se organizó el trabajo a partir de Casos de Usos y de varias iteraciones para obtener los artefactos esperados. Se definió una arquitectura de software orientada micro-servicios con bróker, para soportar una carga alta de trabajo y desacoplar los componentes de software construidos, soportándolo en RabbitMQ como gestor de colas de trabajo y de paso de mensajes. Para evaluar el funcionamiento y el rendimiento se propusieron escenarios de pruebas para el software desarrollado, con el objetivo de obtener datos sobre tiempos de respuesta y capacidad de carga. Se simuló dos escenarios de despliegue de la arquitectura definida. Se establecieron las siguientes pruebas de rendimientos y stress: 1. Carga de activos: Documentos y registro de notas. 2. Carga de Documentos de tamaños mayores a 1 GB. 3. Procesamiento de Hashes. 4. Acceso a la Blockchain. De la ejecución de las pruebas se obtuvo que la plataforma de software responde a las solicitudes con tiempos consistentes acordes a los recursos asignados. Respecto a los documentos se mostró que puede soportar hasta 50 usuarios conectados transaccionando activos digitales de tamaño inferior a 500 MB, situación que se puede ser mejorada con escalamiento vertical u horizontal de los microservicios.

Como conclusiones se puede indicar que las transacciones sobre entornos de Blockchain de tipo público son costosas computacionalmente por sus mecanismos de validación de transacciones, por otro lado, para un entorno privado como lo es Hyperledger Fabric, se observan que los tiempos son bajos y se mantienen constantes ante el aumento de bloques de la Blockchain. Dicha situación se puede explicar por el mecanismo de consenso que requiere de solo unos cuantos nodos validadores, ya que se parte del supuesto del principio de la confianza entre las partes, para el caso en mención se apoyan en el uso de certificados digitales, entidades certificadoras y reglas de validación de acciones. Adicionalmente, se observó que al consultar datos sobre Hyperledger Fabric, proceso que se realiza bajo dos escenarios: World State y el Ledger, en el primer escenario, se evidenció que es útil para acelerar las búsquedas, pero para validar autenticidad, evidenciamos que se debe siempre validar los datos contra el Ledger, ya que es posible generar cambios locales en el World State si no se tienen las validaciones adecuadas, y por lo tanto alterar datos temporalmente.

2. Metodología

A partir del objetivo definido de preservar documentos digitales siguiendo los lineamientos para aplicar el concepto de Preservación a Largo Plazo, se propuso el siguiente esquema de trabajo:

Socialización y asignación de activos digitales: Con los usuarios directamente responsables de salvaguardar la información y partir de entrevistas, se logró identificar los documentos digitales a persistir y se definió realizar el mismo proceso para registrar las notas académicas entregadas por los docentes. A partir de las recomendaciones de AGN y de las reuniones con los actores del proceso, se definió preservar la información de los siguientes activos digitales con su respectiva metadata: Documentos digitales (Archivos con extensión pdf y copias de seguridad de bases de datos de Oracle) y Registros de notas académicas.

Definición de la plataforma de información: A partir de los trabajos de [36], [37], [38] y [39]; y de sus recomendaciones, se definieron tres plataformas de software:

- Persistencia de datos sobre HyperLedger Fabric, ver figura 1. Su objetivo fue persistir la información de los Activos Digitales, garantizando la transparencia y la autenticidad de la información almacenada. Adicionalmente, se definió un Channel para las organizaciones, con sus Nodos Peers y de Ordenamiento, junto con las políticas de validación de transacciones. Para soportar Hyperledger Fabric, se definieron tres organizaciones (ORG1, ORG2 y ORG3), donde se determinó por razones administrativas que la ORG1 y ORG2, serían los nodos validadores de las transacciones. Las credenciales

de las organizaciones fueron generadas por una Autoridad Certificadora (CA) acordada entre las partes y un nodo de ordenamiento para las transacciones.

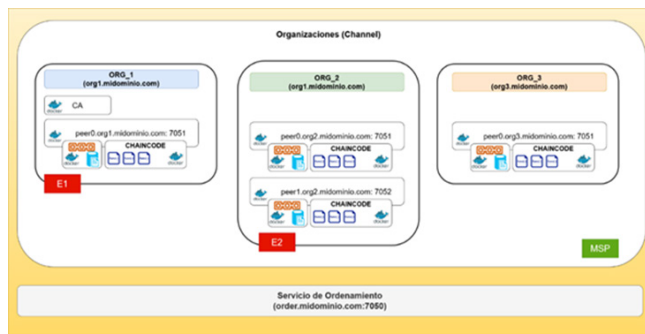


Figura 1. Propuesta de organizaciones en Hyperledger Fabric.

Fuente: Elaboración propia.

Los tipos de datos y procedimientos para representar el concepto de Activo Digital, se definieron en el Chain Code o contrato inteligente ubicado dentro de la Blockchain. Para la implementación del chaincode, este se desarrolló con el lenguaje de programación Go en su versión 1.21.0 y el con API Fabric Gateway v1.5 disponible para las versiones 2.4.4 en adelante.

- Persistencia de documentos sobre un cluster IPFS. Su objetivo fue almacenar el Activo Digital de tipo Documento, apoyándose en un cluster que permite tener la información desagregada en varias máquinas, que para la investigación se definieron 4 nodos. Se optó por almacenar los archivos binarios en IPFS, ya que no es recomendable almacenar archivos binarios en la blockchain. IPFS ofrece facilidad de uso y bajos tiempos de latencia para interactuar con archivos grandes, tal es el caso de las copias de seguridad de las bases de datos.
- Software como servicio para gestionar Activos Digitales, ver figura 2. Su objetivo fue permitir el acceso a los actores del sistema, para interactuar con los Activos Digitales definidos. El software se propuso bajo una arquitectura orientada a microservicios desarrollados sobre el framework de desarrollo Spring Boot, apoyado de un componente de seguridad para la gestión de usuario y de sesiones (KeyCloak), con un gestor de colas de trabajo y de mensajería (Rabbit MQ), y con acceso a datos sobre PostgreSQL y con MongoDB. En RabbitMQ se definieron tres colas de procesamiento: Documentos pesados. Gestiona activos con tamaños superiores a 1 GB y 5 GB. Documentos livianos. Gestiona activos con tamaños inferiores a 1 GB. Notas. Gestiona activos relacionados con el registro de notas académicas, los cuales no superan un 1 Mb de información. Adicionalmente, se utilizó un componente de Observabilidad para medir y visualizar el rendimiento del de la plataforma.

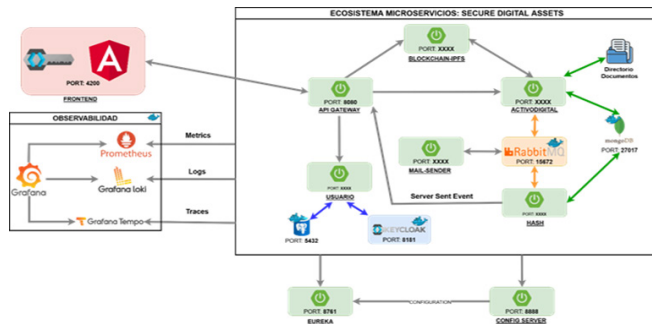


Figura 2. Arquitectura de Microservicios.

Fuente: Elaboración propia.

Asignación de hash: Se propuso que para cada activo digital se generan los siguientes hashes: Hash de activo (activo) y Hash con metadata (activo + metadata). De tal manera, que a partir de los hashes generados fuese posible identificar si un activo ya existe, o si existe, saber que metadata le han adicionado.

Desarrollo de pruebas: Se propusieron escenarios de pruebas con el objetivo de medir el rendimiento en términos de carga y de stress, ya que era necesario conocer la respuesta del sistema ante posibles escenarios de múltiples usuarios conectados y procesando activos, lo cual significa evaluar el rendimiento del sistema bajo condiciones esperadas, y adicionalmente, se propuso conocer en qué puntos el sistema puede fallar ante una demanda alta de servicios o bajo condiciones extremas. Para la ejecución de pruebas se utilizó un servidor HP ProLiant ML110 Gen9 con las siguientes características: Procesador Intel Xeon con 12 núcleos, 64 GB de RAM, disco SATA de 2 TB, y un sistema operativo Ubuntu 22.04. Dentro del servidor se configuró una máquina virtual basada en kernel (KVM) con QEMU, dicha máquina virtual fue configurada con los siguientes recursos: 6 núcleos del procesador, 140 GB de disco virtual; sistema operativo Ubuntu 22.04; respecto a la memoria RAM, fue variable según el escenario de prueba: 16 GB para el escenario número 1 y 32 GB para el escenario número 2.

Las pruebas fueron ejecutadas con la herramienta Jmeter para enviar las peticiones concurrentes por parte de los usuarios a los servicios definidos; por otra lado, se realizaron los cálculos de tiempos de procesamiento a nivel de generación de hashes y de consulta a la blockchain, entiendo que Hyperledger Fabric permite consultar la información en dos lugares diferentes: world state y la blockchain. Se propuso enviar a la plataforma peticiones a los servicios que se habilitaron para manejar activos: documentos y registro de notas académicas. Se definieron escenarios con variaciones en la cantidad de activos y el número de usuarios que realizan transacciones (5, 10, 25 y 50). Las pruebas fueron realizadas con la misma máquina virtual, pero con variación de la memoria RAM. Se organizaron pruebas a nivel de: Pruebas de carga: Documentos con tamaño variable, Sabanas de Notas académicas, procesamiento de hashes y consulta información al World State de la blockchain y Pruebas de stress:

Documentos de gran tamaño (mayores o iguales a 1 GB) y consulta de información histórica o records de la blockchain.

3. Resultados

En las transacciones realizadas sobre la plataforma de Gestión de Documentos, se observa que los tiempos de acceso son bajos y se mantienen constantes ante el aumento de documentos livianos (<=10MB) en los dos escenarios. La tabla 1 y 2, muestran algunos datos de la pruebas realizadas:

Etiqueta	Cantidad de Muestras	Tiempo (ms)	Cantidad de Muestras	Tiempo (ms)	Cantidad de Muestras	Tiempo (ms)	Cantidad de Muestras	Tiempo (ms)
Documento PDF 400KB	5	349	10	390	25	627	50	1163
Documento PDF 1MB	5	463	10	403	25	700	50	1247
Documento PDF 3MB	5	523	10	589	25	1053	50	1748
Documento PDF 10MB	5	525	10	755	25	1538	50	2382

Tabla 1. Pruebas de documentos livianos – escenario uno.

Fuente: Elaboración propia.

Etiqueta	Cantidad de Muestras	Tiempo (ms)	Cantidad de Muestras	Tiempo (ms)	Cantidad de Muestras	Tiempo (ms)	Cantidad de Muestras	Tiempo (ms)
Documento PDF 400KB	5	251	10	287	25	523	50	1299
Documento PDF 1MB	5	343	10	369	25	627	50	1278
Documento PDF 3MB	5	476	10	526	25	1039	50	1726
Documento PDF 10MB	5	672	10	767	25	1467	50	2306

Tabla 2. Pruebas de documentos livianos – escenario dos.

Fuente: Elaboración propia.

En relación a los documentos pesados (>=1GB), solo hay datos con 5 usuarios simultáneos con documentos pesados, ya que los dos escenarios de pruebas no soportaron más carga de trabajo, ya que los recursos asignados no fueron suficientes. La figura 3 y 4 muestran información acerca de la carga de datos:

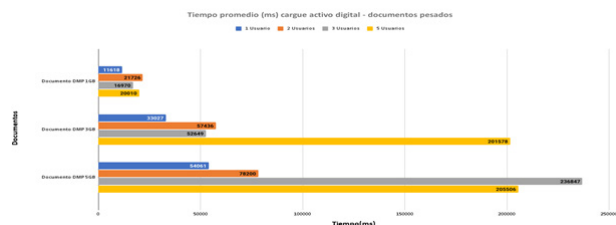


Figura 3. Carga de documentos pesados, escenario 1.

Fuente: elaboración propia.

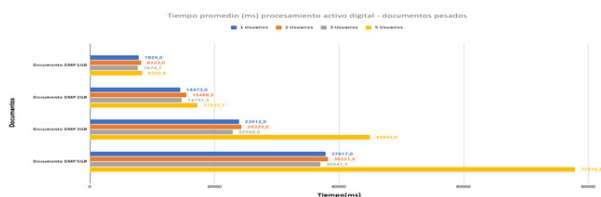


Figura 4. Carga de documentos pesados, escenario 2.

Fuente: elaboración propia.

Finalmente, se realizaron pruebas directamente a Hyperledger Fabric, para conocer su comportamiento respecto al proceso de registro de activos, acceso a datos al World State y al Ledger. Las pruebas fueron realizadas en el escenario uno que tiene menos recursos de hardware asignados. Se obtuvieron los siguientes datos:

Registrar Activo	Cantidad de Muestras	Tiempo (ms)	Tiempo (ms) Min	Tiempo (ms) Máx	Tiempo (ms) Desv. Estándar	Rendimiento
Registro activo digital 1	5	1521	1123	1921	283.3	2.6/sec
Registro activo digital 2	10	1582	791	3245	831.97	2.4/sec
Registro activo digital 3	25	1800	1057	3327	831.79	6.4/sec
Registro activo digital 4	50	2651	1213	4073	785.6	11.0/sec

Tabla 3. Registrar Activo en HyperLedger Fabric.

Fuente: elaboración propia.

Número de activos registrados	Tiempo de respuesta (ms)			
	5 usuarios	10 usuarios	25 usuarios	50 usuarios
1000	38	40	102	363
2000	85	98	278	422
5000	26	30	91	330
10000	29	33	77	394

Tabla 4. Consultas al World State de Hyperledger Fabric.

Fuente: elaboración propia.

Número de activos registrados	Tiempo de respuesta(ms)			
	5 usuarios	10 usuarios	25 usuarios	50 usuarios
1000	32	35	80	309
2000	44	45	101	338
5000	29	28	69	302
10000	24	66	85	312

Tabla 5. Consultas libro mayor (Ledger) o record de Hyperledger Fabric.

Fuente: elaboración propia.

4. Conclusiones.

Las transacciones sobre entornos de blockchain de tipo público son costosas computacionalmente por sus mecanismos de validación de transacciones o mecanismo de consenso, que se apoyan en la minería, los cuales se ven reflejadas en los aumentos en los tiempos de respuestas, como los indican los trabajos de [20] y [21], para el caso Hyperledger Fabric se observa que los tiempos son bajos y se mantienen constantes ante el aumento de bloques de la cadena, como se observó en los datos de las pruebas realizadas. Dicha situación se puede explicar por el mecanismo de consenso que requiere de solo unos cuantos nodos validadores, ya que el principio de las blockchain de tipo privado es la confianza entre las partes.

Al consultar datos sobre Hyperledger Fabric, proceso que se realiza bajo dos escenarios: World State y el Ledger de la Blockchain, en el primer escenario, es útil para acelerar las búsquedas, pero para validar autenticidad, evidenciamos que se debe siempre validar los datos contra el Ledger, ya que es posible generar cambios locales en el World State si no se tienen las validaciones adecuadas, y por lo tanto alterar datos temporalmente.

La arquitectura de software basada en microservicios que se propuso para la gestión de Activos Digitales respondió eficientemente en relación a los recursos ofrecidos para los escenarios planteados. Se observó que la delegación de trabajo en un gestor de colas permitió recibir activos de tamaño pequeño como de tamaño grande, y procesarlos satisfactoriamente, sin afectar el servicio de la plataforma.

La plataforma tiene un límite de procesamiento de Activos Digitales de tamaños de 25 GB para 5 usuarios concurrentes, situación presentada por las limitaciones de memoria RAM de los dos escenarios de prueba, para mejorar las prestaciones de procesamiento se recomienda aumentar la RAM del microservicio que procesa los Activos o desplegar el microservicio en otra máquina.

En el proceso de consultas de datos al World State y al Ledger, se observó que la HyperLedger utiliza un cache para optimizar las consultas, por ese motivo en las pruebas se enviaron consultas aleatorias, para evitar respuestas pre-guardadas, de tal forma de tener valores más reales en los tiempos de respuestas.

La persistencia de la información asociada a los Activos Digitales en dos

escenarios (Hyperledger Fabric e IPFS), permitió optimizar el uso y acceso a los activos, generando tiempos de respuestas y de procesamientos más pequeños, acorde a lo expresado en [27] y [28].

5. Reconocimientos

Este trabajo fue financiado por la Universidad de los Llanos bajo el proyecto C03-F02-012-2022. Los autores expresan sus agradecimientos a la Universidad de los Llanos, a la Dirección General de Investigaciones y a los miembros del grupo de investigación GITECX por su colaboración, orientación y apoyo logístico, lo cual hizo posible esta investigación.

6. Referencias

[1] A. G. D. E. L. A. N. AGN, "Política Pública de Archivos," 2016. [Online]. Available: <http://archivogeneral.gov.co>

[2] C. C. de Informatica y Telecomunicaciones, "Tendencias del Cibercrimen 2021-2022," Jul. 2021. [Online]. Available: <https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-2021-2022-nuevas-amenazas-al-comercio-electronico/>

[3] D. Arias, "Colombia sufrió 1.000 millones de ataques en el primer trimestre," Jul. 2021. [Online]. Available: <https://www.enter.co/empresas/seguridad/colombia-sufrio-1-000-millones-de-ataques-en-el-primer-trimestre/>

[4] ACIS, "Tres de cada 10 víctimas de ransomware en Colombia paga el rescate, pero solo una de estas recupera sus datos," Jul. 2021. [Online]. Available: <https://www.acis.org.co/portal/content/noticiasdelsector/tres-de-cada-10-v%C3%ADctimas-de-ransomware-en-colombia-paga-el-rescate-pero-solo-una-de-estas>

[5] Semana, "Colombia es blanco del 30 por ciento de los ataques de ransomware de América Latina. ¿Cómo puede proteger su empresa?," Semana.com, [Online]. Available: <https://www.semana.com/mejor-colombia/articulo/colombia-es-blanco-del-30-por-ciento-de-los-ataques-de-ransomware-de-america-latina-como-puede-proteger-su-empresa/202148/>

[6] xataka.com.co and J. Tamayo, "Colombia es uno de los países más atacados cibernéticamente, revela estudio ," Jul. 2017. [Online]. Available: <https://www.xataka.com/seguridad/colombia-es-uno-de-los-paises-mas-atacados-ciberneticamente-revela-estudio>

[7] de la República Congreso, "Ley 1955 - Plan Nacional de Desarrollo 2018-2022," 2019.

[8] M. de Tecnologías de la Información y las Comunicaciones MinTIC, "Guía de Referencia de Blockchain para la Adopción e Implementación de Proyectos en el Estado Colombiano," 2020.

[9] V. L. Lemieux, "Blockchain Technology for Recordkeeping, Help or Hype?," 2016. doi: 10.13140/RG.2.2.21736.67842.

[10] E. García-Morales, "Luces y sombras sobre el impacto del blockchain en la gestión de documentos," Anuario ThinkEPI, vol. 12, pp. 345-351, 2018, doi: 10.3145/thinkepi.2018.58.

[11] C. B. Ruesta, "TRANSFORMACIÓN DIGITAL DESDE LA PERSPECTIVA DE LA GESTIÓN DOCUMENTAL," RUIDERAe, vol. 13, no. ISSN 2254-7177, 2018, [Online]. Available: <https://revista.uclm.es/index.php/ruiderae/article/view/1834>

[12] U. O. C.-M. y Publicidad, "¿Qué es un activo digital y por qué es importante para una empresa?," Jul. 2020. [Online]. Available: <https://fp.uoc.fje.edu/blog/que-es-un-activo-digital-y-por-que-es-importante-para-una-empresa/>

[13] P. A. Management, "Qué son los activos digitales y cómo invertir en ellos," Jul. 2023. [Online]. Available: <https://am.pictet/es/blog/articulos/innovacion/activos-digitales-como-invertir>

[14] wikipedia.org, "Activo digital," Jul. 2024. [Online]. Available: https://es.wikipedia.org/wiki/Activo_digital

[15] S. D. Palma, R. Pareschi, and F. Zappone, "What is your Distributed (Hyper)Ledger?," in 2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 2021, pp. 27-33. doi: 10.1109/WETSEB52558.2021.00011.

[16] Sammeta and L. Parthiban, "Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis

- model,” *Complex & Intelligent Systems*, 2021, doi: 10.1007/s40747-021-00549-w.
- [17] M. Uddin, “Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry,” *Int J Pharm*, vol. 597, p. 120235, 2021, doi: <https://doi.org/10.1016/j.ijpharm.2021.120235>.
- [18] L. Li, Z. Yue, and G. Wu, “Electronic Medical Record Sharing System Based on Hyperledger Fabric and InterPlanetary File System,” in 2021 The 5th International Conference on Compute and Data Analysis, Association for Computing Machinery, 2021, pp. 149–154. doi: 10.1145/3456529.3456555.
- [19] S. Ambler, *Agile Modeling: Effective Practices for eXtreme Programming and the Unified Process*, 1st ed. Wiley, 2002.
- [20] J. Clavin et al., “Blockchains for Government: Use Cases and Challenges,” *Digit. Gov.: Res. Pract.*, vol. 1, no. 3, Jul. 2020, doi: 10.1145/3427097.
- [21] V. L. Lemieux, “Blockchain and Recordkeeping: Editorial,” *Computers*, vol. 10, no. 11, 2021, doi: 10.3390/computers10110135.
- [22] J. Zou, D. He, S. Zeadally, N. Kumar, H. Wang, and K. R. Choo, “Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges,” *ACM Comput. Surv.*, vol. 54, no. 8, Jul. 2021, doi: 10.1145/3456628.
- [23] A. I. Sanka and R. C. C. Cheung, “A systematic review of blockchain scalability: Issues, solutions, analysis and future research,” *Journal of Network and Computer Applications*, vol. 195, p. 103232, 2021, doi: <https://doi.org/10.1016/j.jnca.2021.103232>.
- [24] S. Olnes and A. Jansen, “Blockchain Technology as Infrastructure in Public Sector: An Analytical Framework,” in Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, in dg.o '18. New York, NY, USA: Association for Computing Machinery, 2018. doi: 10.1145/3209281.3209293.
- [25] P. Sharma, R. Jindal, and M. D. Borah, “Blockchain Technology for Cloud Storage: A Systematic Literature Review,” *ACM Comput. Surv.*, vol. 53, no. 4, 2020, doi: 10.1145/3403954.
- [26] H. Huang, J. Lin, B. Zheng, Z. Zheng, and J. Bian, “When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues,” *IEEE Access*, vol. 8, pp. 50574–50586, 2020, doi: 10.1109/ACCESS.2020.2979881.
- [27] H.-S. Huang, T.-S. Chang, and J.-Y. Wu, “A Secure File Sharing System Based on IPFS and Blockchain,” in Proceedings of the 2020 2nd International Electronics Communication Conference, in IECC 2020. New York, NY, USA: Association