UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

Modelo distribuido para la seguridad de datos en corresponsales no bancarios basado en Blockchain

Trabajo de titulación previo a la obtención del
Título de Ingeniero de Sistemas

AUTOR: Sergio Ignacio Gavino Merino

TUTOR: Joe Frand Llerena Izquierdo

Guayaquil – Ecuador

2024

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Sergio Ignacio Gavino Merino con documento de identificación N° 0924098825 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 22 Julio del año 2024

Atentamente,

_____

Sergio Ignacio Gavino Merino

0924098825

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Sergio Ignacio Gavino Merino con documento de identificación N° 0924098825, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo Académico: "Modelo distribuido para la seguridad de datos en corresponsales no bancarios basado en Blockchain", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 22 Julio del año 2024

Atentamente,

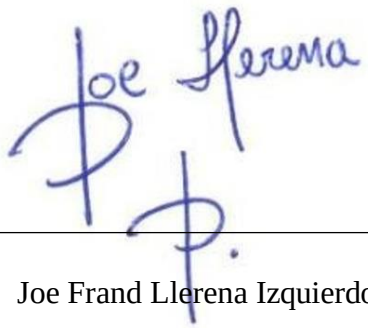
Sergio Ignacio Gavino Merino
0924098825

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: Modelo distribuido para la seguridad de datos en corresponsales no bancarios basado en Blockchain, realizado por Sergio Ignacio Gavino Merino con documento de identificación N° 0924098825, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 22 Julio del año 2024

Atentamente,



Joe Frand Llerena Izquierdo
0914884879

DEDICATORIA

Dedico este trabajo a mi familia, a mi mama, a mi papa y a mi hija por siempre darme la fuerza y la motivación cada día apoyándome en esta etapa de mi vida que no ha sido fácil, pero ha llegado el día donde todo el esfuerzo que han hecho por mi ha dado los frutos, También quiero agradecer a Dios por darme la sabiduría y las ganas de seguir adelante a pesar de los obstáculos que he tenido en este camino universitario.

También quiero dedicar este trabajo a todos mis compañeros de universidad que he cosechado durante estos años que de una u otra manera han ayudado en este camino univeritario.

AGRADECIMIENTO

- Agradezco a mi Tutor de Articulo Académico, al Ing. Joe Frand Llerena Izquierdo, por su paciencia y grandes consejos a lo largo de este articulo académico que sin el este Articulo no existiría, muchas gracias, profesor.
- Agradezco a todos los profesores de la Carrera de Ingeniería en Sistemas que me enseñaron de forma academia y personal grandes valores humanos para poder afrontar retos que se han cruzado en mi carrera profesional.

RESUMEN

Las transacciones generadas por los Corresponsales No Bancarios tienen una mejor alternativa para optimizar la transparencia y la seguridad; otros problemas son problemas de tarifas, escalabilidad y privacidad. Blockchain es una tecnología que soluciona en forma potencial aquellos problemas por sus características como la inmutabilidad, la trazabilidad, el no repudio y la descentralización. El objetivo general de esta investigación es diseñar un modelo distribuido para la seguridad de datos en Corresponsales No Bancarias basado en Blockchain. En la metodología se emplea una revisión de la literatura, la investigación empírico-analítico, el enfoque cualitativo y la técnica de la observación. Entre los resultados se conoció que, los principales componentes de la seguridad en Blockchain son la Transparencia, Integridad, Confiabilidad, Disponibilidad, Trazabilidad y Privacidad. El modelo diseñado en esta investigación consta de cinco secciones: Clientes, Red de Corresponsales No Bancarios, Red de Transmisión, Banco y Entidades de Control. La viabilidad y aplicabilidad mediante la estrategia Blockchain integrada, tiene 16 factores, de los cuales dos factores son críticos, dos factores se deben mejorar y doce factores son ideales en el modelo propuesto. Se concluyó que la transparencia, la trazabilidad, la seguridad y la inmutabilidad están garantizadas en el modelo gracias a la tecnología Blockchain, y el modelo está diseñado sobre Hyperledger para gestionar las transacciones en forma privada, es decir entre los interesados como los Corresponsales No Bancarios, Bancos y Entidades de Control Ecuatoriano.

Palabras claves: Corresponsales No Bancarios, Modelo distribuido, Blockchain, Hyperledger.

ABSTRACT

Transactions generated by Non-Banking Correspondents have a better alternative to optimize transparency and security; other issues include pricing, scalability, and privacy issues. Blockchain is a technology that potentially solves those problems due to its characteristics such as immutability, traceability, non-repudiation and decentralization. The general objective of this research is to design a distributed model for data security in Non-Banking Correspondents based on Blockchain. The methodology uses a literature review, empirical-analytical research, a qualitative approach and an observation technique. Among the results, it was known that the main components of Blockchain security are Transparency, Integrity, Reliability, Availability, Traceability and Privacy. The model designed in this research consists of five sections: Customers, Non-Banking Correspondents' Network, Transmission Network, Bank and Control Entities. The feasibility and applicability through the integrated Blockchain strategy has 16 factors, of which two factors are critical, two factors must be improved, and twelve factors are ideal in the proposed model. It was concluded that transparency, traceability, security and immutability are guaranteed in the model thanks to Blockchain technology, and the model is designed on Hyperledger to manage transactions privately, that is, between interested parties such as Non-Banking Correspondents, Banks and Ecuadorian Control Entities.

Key words: Non-Banking Correspondents, Distributed Model, Blockchain, Hyperledger.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

En la actualidad, las herramientas informáticas monetarias están subsistiendo sin soluciones y se vuelven obsoletas; los productos, servicios bancarios y otras soluciones pueden brindar mejor transparencia. Además, las transacciones bancarias no pueden tener un rastro para seguimiento, o son fáciles de corromper o no utilizan criptografía. Se necesita diseñar sistemas seguros de transferencia de valores, acelerar los procesos de negocio, generar nuevos procesos, mantener la transparencia, facilitar la auditoría, y también es necesario aumentar la confianza. Existen actores financieros que mantienen inadecuada infraestructura, deben evaluar sus prioridades y optimizar sus prácticas comerciales. Las transacciones que llegan desde agencias no bancarias tienen el riesgo de duplicación de datos, latencia en el movimiento de liquidez, muchas comisiones y otros obstáculos que pueden entorpecer el seguimiento o auditoría para los reguladores del gobierno. En un entorno financiero pueden existir muchos intermediarios financieros y terceros, como los bancos centrales, depositarios concentrados de valores, organizaciones de compensación, sistemas congregados de gestión de garantías, entre otros (Dashkevich et al., 2020).

Existe gran cantidad de intermediarios en diferentes lugares y horarios durante el proceso de banca corresponsal a nivel local e internacional, algunos problemas latentes son: los sistemas de pago interbancarios no mantienen transacciones seguras ni privadas ni rentables (M. Islam et al., 2023).

De acuerdo a (Saputhanthri et al., 2022), existen varios problemas en la realización de pagos y mercados como son: problemas de tarifas, escalabilidad, problemas de seguridad y privacidad (Zerega-Prado & Llerena-Izquierdo, 2022); y Blockchain es una tecnología que soluciona en forma potencial aquellos problemas por sus características como la inmutabilidad, la trazabilidad, el no repudio y la descentralización (Melendrez-Caicedo & Llerena-Izquierdo, 2022). Otros problemas existentes son: los sistemas de pagos están basados en bases de datos centralizadas que pueden ser atacadas, otro problema es la escalabilidad que ciertas bases de datos no soportan, algunas bases de datos soportan una máxima cantidad de registros por su licencia libre, otras bases de datos son caras en relación a su utilidad (Papadis & Tassiulas, 2020). No existe equidad de los sistemas en la protección de los datos, no existen reglas en los sistemas o no se garantiza la implementación de las reglas; algunos sistemas permiten visualizar información confidencial en las transacciones, y puede existir manipulación de los datos; la

información de las transacciones puede ser divulgada, otros sistemas visualizan la identidad de los clientes o inversores (Chang & Wang, 2023).

Blockchain es una tecnología disruptiva y tiene impacto en áreas; la industria bancaria está aprovechando y cada evento digital es compartido entre múltiples participantes, la industria bancaria quiere aprovechar los componentes de esta tecnología.

La tecnología Blockchain se utiliza en diferentes áreas como: educación en exámenes en línea para evaluación en cursos estudiantiles que determinan su progreso (Abdelsalam et al., 2024), energía eléctrica (De Villiers & Cuffe, 2020), gestión en la donación de sangre (Hawashin et al., 2021), en la cadena de suministro para garantizar la trazabilidad y seguridad de productos (Zhang & Ling, 2023), sistemas de pagos (Hu et al., 2021), atención sanitaria biomédica, computación en la nube, gestión de identidad, marketing, turismo, agricultura, internet de las cosas, voto electrónico (Tran et al., 2021), sistemas de gobierno, caridad, seguro privado, ciber seguridad, pronóstico (Jabbar et al., 2022).

En Ecuador existen Corresponsales No Bancarios, es decir son locales comerciales que no pertenecen al banco, por ejemplo: Banco de Guayaquil tiene más de 19 mil puntos de atención (Banco de Guayaquil, 2024), Banco del Pichincha tiene más de 7 mil puntos de atención (Banco del Pichincha, 2024), Banco del Pacífico tiene más de 14 mil puntos de atención (Banco del Pacífico, 2024), Banco de Loja tiene más de 4 mil puntos a nivel nacional (Banco de Loja, 2024).

Si se aplica la tecnología Blockchain, continua el dinero efectivo tradicional y se utilizan los sectores públicos y privados, porque facilita una trazabilidad rápida e impecable del flujo monetario, y además de realizar auditoría rentable, se mantiene la privacidad y seguridad. El sector bancario y sector de pagos ofrece dirección a servicios financieros, y es posible incluir áreas o zonas o países sin aplicaciones bancarias tradicionales; las transacciones de pagos y otras operaciones bancarias desde agencias o locales no bancarias se facilitan, son eficientes y seguras (M. M. Islam & In, 2023).

Un enfoque de Blockchain en las finanzas son los pagos, la compensación y la liquidación, esta tecnología mantiene programas llamados Smart Contract. Blockchain logra que los participantes hagan sus transacciones sin mantener una autoridad central y mantener un ledger (repositorio de datos) que registre las transacciones (Farrell, 2019).

Se propone el diseño de una red Blockchain que puede ayudar en la reducción de la complejidad, transparentar la disponibilidad de fondos, garantizar la inmutabilidad de las transacciones, optimizar la resiliencia de la red a través de la gestión de datos distribuidos, y minimizar el riesgo operativo y financiero.

El objetivo general es diseñar un modelo distribuido para la seguridad de datos en Corresponsales No Bancarias basado en Blockchain.

Objetivos específicos:

- Analizar modelos distribuidos para la categorización de los movimientos bancarios mediante una revisión de la literatura.
- Diseñar un modelo distribuido para la seguridad de datos generados en corresponsales no bancarias basado en tecnología Blockchain.
- Evaluar el modelo distribuido para la estimación de la viabilidad y aplicabilidad mediante la estrategia Blockchain integrada.

Aunque existen autores que recomiendan mejorar la practicidad en Blockchain, es decir, sobresalir en las limitaciones tecnológicas, porque blockchain contiene un proceso de toma de decisiones descentralizado con datos que son más extensos.

2. REVISIÓN DE LITERATURA

La tecnología de Blockchain, es un conjunto de transacciones compartidas e inmutables que mantienen una marca de tiempo y se guardan en bloques cronológicos con un hash único. Los bloques están enlazados en forma criptográfica y son verificables por medio de la red distribuida. La red mantiene un algoritmo de consenso para coincidir en una única verdad. Las transacciones no se pueden modificar, sino toda la cadena se vuelve incorrecta. Se clasifican en dos categorías: sin permiso y con permiso. Sin permiso todo nodo con una copia es un validador y anuncia su consenso; Con permiso solo los nodos autorizados anuncian su consenso y realizan transacciones (M. M. Islam & In, 2023).

Entre los componentes de Blockchain se tiene:

Distributed ledgers: Registro descentralizado, replicado, sincronizado y comparte las transacciones que se realizan entre los participantes de la cadena a través de un sellado criptográfico. En el Ledger, existen nodos que no confían en otros nodos y las transacciones son verificadas. Un Ledger disminuye la participación de intermediarios.

Smart Contract: Constituye las reglas entre todos los participantes de la cadena. Un Smart Contract son programas informáticos que avalan las transacciones en sus acuerdos legales y que los registros gestionados por el Ledger posean autoridad. Al momento de existir cambios en los activos de datos, se activan los términos del SC, además se automatizan las leyes y estatutos (Youn & Cho, 2021).

De acuerdo a (Saputhanthri et al., 2022) existen 4 plataformas Blockchain:

- Pública: Cualquier persona y sin permiso accede a la red, y es un nodo que valida las transacciones. Ejemplo: Etereum y Bitcoin.
- Privada: Los permisos y el acceso a la red solo pertenecen a usuarios autorizados. Ejemplo: Multichain y Hyperledger.
- Consorcio: o Federado, aquí varias organizaciones gobiernan la red. Ejemplo: R3
- Híbrida: Mantienen procesos públicos y privados de acuerdo con la transacción en la red pública. Ejemplo: Ripple.

Varios autores proponen un sistema de pago digital y aplica verificación distribuida (Hu et al., 2021); se utiliza en aldeas rurales que se mantienen interconectadas a Internet pública, y estas

clases de conexiones no son confiables. Se utiliza Ethereum, Smart contract realiza el inicio de cuentas de usuario, las interacciones entre operador de crédito y clientes. Se identifican áreas de aplicaciones IoT, como salud, agricultura, vehículos, fabricación inteligente, comercio y finanzas; utilizaron Blockchain para asegurar los datos y privacidad (Saputhanthri et al., 2022).

Otros autores proponen a Blockchain como una gestión de moneda y pagos en moneda digital en forma transparente, auditable y con privacidad; utilizan claves públicas para recibir un pago y no se revela el saldo del remitente; además garantizan el cumplimiento normativo en una red de moneda digital (M. M. Islam & In, 2023). Además como un sistema de pago transfronterizo utiliza Blockchain Consorcio para fluir y bajar costos de transacciones que sean auditables, el enfoque protege la privacidad de los clientes y certifica la transparencia (M. Islam et al., 2023).

En otros trabajos, se introduce las redes de canales de pago para que las transacciones se realicen en forma segura entre los participantes y no sobrecargar la red; se destaca las operaciones en las redes de canales de pago, los autores afirman que está al alcance de las economías (Papadis & Tassiulas, 2020). Además de la construcción de un modelo para bancos y empresas, utilizan el incentivo crediticio y el mecanismo de castigo para optimizar el financiamiento (Zhao et al., 2022).

3. METODOLOGÍA

Para esta propuesta se emplea una Revisión de la Literatura (Touloupou et al., 2022) que es un análisis de artículos disponibles. Se verificaron requisitos antes de la exploración. La figura 1 presenta las fases de la revisión de la literatura. 1) Fase Planificación presenta la necesidad de realizar la revisión, el protocolo de revisión que es definir las preguntas de investigación, definir las librerías, definir las palabras claves, y evaluar ese protocolo. 2) Fase Realización, se busca en las librerías, se seleccionan artículos, se utiliza criterios de inclusión-exclusión, y se extraen los datos desde los artículos para asentarlos en una hoja electrónica. 3) Fase Presentación, analiza y presenta los datos extraídos, se presentan cuadros estadísticos que responden las preguntas de investigación.

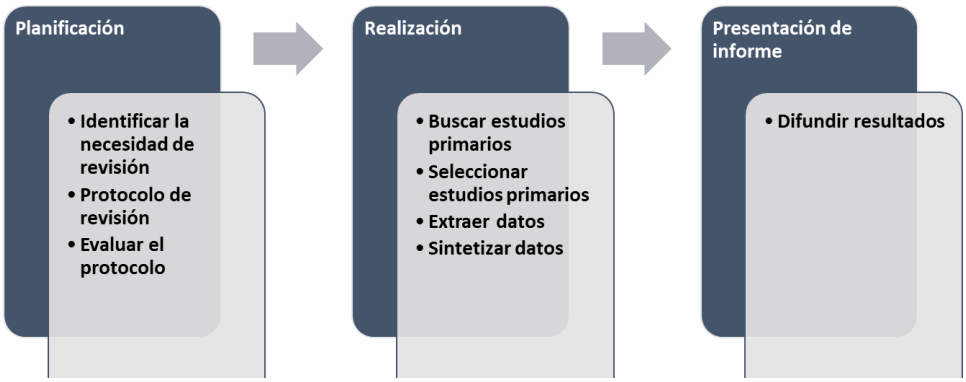


Figura 1. Revisión de la literatura.

Se definieron las siguientes preguntas de investigación, que serán respondidas en la fase resultados en este documento de investigación.

1. ¿Qué componentes de seguridad cubre Blockchain?
2. ¿Qué componentes de Blockchain se encuentran en los artículos?
3. ¿En qué áreas se utiliza Blockchain?
4. ¿Qué herramientas de software se utilizan?
5. ¿Qué clase de diagramas se presentan en los artículos?
6. ¿Qué plataformas se utilizan en los modelos Blockchain?
7. ¿Otras tecnologías adicionales se utilizan con Blockchain?

En el diseño de un modelo distribuido para la seguridad de datos en Corresponsales No Bancarias. Se utiliza la investigación empírico-analítico que considera la factibilidad de una solución por medio de evidencias empíricas. Se utiliza el enfoque cualitativo para el modelo. Se utiliza la técnica de la observación de otros modelos o arquitecturas distribuidas en Blockchain. Se utiliza gráficos para presentar el modelo y su descripción.

En la evaluación del modelo distribuido para la estimación de la viabilidad y aplicabilidad, se utilizan los siguientes indicadores numéricos.

- Análisis de uso: Prueba de existencia, Prueba de no existencia, Prueba de orden, Prueba de identidad, Prueba de autoría.
- Análisis de naturaleza y viabilidad: Cumple los requisitos de uso de la cadena, Tipo de cadena se utiliza, Utilidad de la aplicación, Se compensa a los nodos por los recursos, Grado de desarrollo del negocio.
- Evaluación de potencialidad e interés: Justificable, Escalable, Extrapolable, Persistente, Desarrollo, Aceptable.

4. RESULTADOS

4.1. Análisis de modelos distribuidos para la categorización de los movimientos bancarios mediante una revisión de la literatura

De un total de 117 artículos obtenidos de las bibliotecas IEEE Xplore y ACM Digital Library, luego se descartaron 8 artículos por ser duplicados, luego se aplicaron los criterios de inclusión y exclusión, se descartaron 26 artículos. Luego se descartaron 17 artículos ilegibles porque no coinciden con Blockchain ni coinciden con Banca; en cambio otros presentan el resumen o no tienen Blockchain relacionado a la banca financiera, otros no son acceso libre. Otros 31 documentos se descartaron porque son pagados, libros, poster, no idioma inglés; luego se obtuvieron 35 documentos para lectura integra y se descartaron 11 artículos porque son lectura gris o no fueron específicos en los modelos o no se pueden utilizar en esta investigación. Finalmente, el resultado general son 24 artículos útiles para los fines de esta investigación, que se presentan en la tabla 1.

Tabla 1. Artículos seleccionados

Biblioteca	Artículos	Cantidad
IEEE Xplore	(Abdelsalam et al., 2024), (De Villiers & Cuffe, 2020), (Hawashin et al., 2021), (Zhang & Ling, 2023), (Hu et al., 2021), (Saputhanthri et al., 2022), (M. M. Islam & In, 2023), (Ma et al., 2022), (M. Islam et al., 2023), (Tran et al., 2021), (Kimura et al., 2024), (Papadis & Tassiulas, 2020), (Chang & Wang, 2023), (Jabbar et al., 2022), (Zhao et al., 2022)	18
ACM Digital Library	(Syed et al., 2020), (Bhutta et al., 2021), (Alzhrani et al., 2022), (Agrawal et al., 2022), (Lee & Kim, 2022), (Al-Shaibani et al., 2020), (Chaleenutthawut et al., 2024), (Chen et al., 2022)	8
	Total	24

Fuente: Autoría propia.

Estos 24 artículos fueron tabulados en una hoja electrónica, en cada columna están los factores agrupados de acuerdo con las preguntas de investigación, que son los siguientes. Grupo Componentes de Seguridad con los factores: Confiabilidad, Integridad, Disponibilidad, Transparencia, Trazabilidad y Privacidad. Grupo Componentes de Blockchain con los factores: Smart Contract, Ledger DB, Concenso y Certificados de autenticación. Grupo Áreas con los factores: Educación, Energía Eléctrica, Salud, Productos y Finanzas. Grupo Herramientas con los factores: Ethereum, Solidity e Hyperledger. Grupo Clase de Diagramas con los factores: Diagramas de Secuencia, Diagrama de Datos, Diagrama de Arquitectura y Algoritmos. Grupo

Plataformas con los factores: Pública, Privada, Consorcio y Híbrida. Grupo Otras tecnologías con los factores: Internet de las Cosas e Inteligencia Artificial.

Por cada uno de los 24 artículos seleccionados, se tabularon dentro de los factores, cada factor se suma y se obtiene el porcentaje con relación a los 24 artículos. Las siete preguntas de investigación que se presentaron en la metodología se responden en esta sección, cada pregunta representa cada grupo de factores y se presenta un gráfico de barras en porcentajes.

4.1.1 ¿Qué componentes de seguridad cubre Blockchain?

Se hallaron seis componentes de seguridad como: Confiabilidad en 15%, Integridad en 19%, Disponibilidad en 16%, Transparencia en 21%, Trazabilidad en 13%, Privacidad en 16%. Esto quiere decir que, en las arquitecturas de los artículos, la transparencia e integridad son los más importantes o mejor considerados, los demás factores también son importantes y son cubiertos por Blockchain. En Blockchain no es necesario la participación de terceros para preservar los estándares de transparencia y evadir la posible falsificación, esta tecnología verifica las transacciones. En Blockchain, los participantes acceden a las transacciones que están almacenadas en el ledger que se garantiza la privacidad e integridad, ver figura 2.

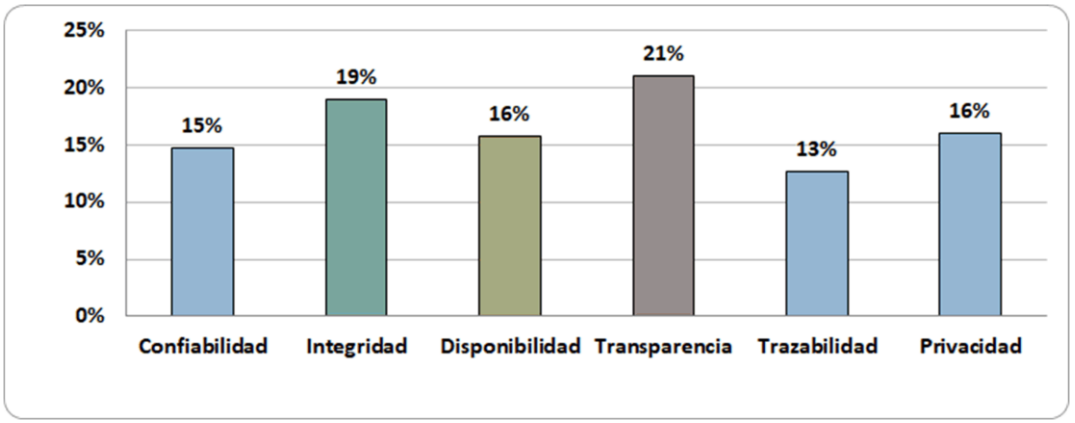


Figura 2. Factores de seguridad.

4.1.2 ¿Qué componentes de Blockchain se encuentran en los artículos?

Se hallaron cuatro componentes de Blockchain como: Smart Contract en 33%, Ledger DB en 25%, Consenso en 21%, Certificados de autenticación en 21%. Esto quiere decir que, la mayoría de los documentos presentan la importancia de explicar la implementación del SC. Los Smart Contract realizan el monitoreo, seguimiento, automatización y control de ejecuciones de los procesos, permiten cumplir las condiciones del proceso. Existe beneficio en utilizar el SC en la

banca, gobierno, seguros y cadena de suministro. El SC genera arquitecturas descentralizadas en esquemas de comunicación interesantes que simplifican la comunicación para generar y consumir eventos. Aunque existen ciertas áreas de desafíos técnicos afines a la disponibilidad, seguridad, solidez, la privacidad y considerar aspectos legales, ver figura 3.

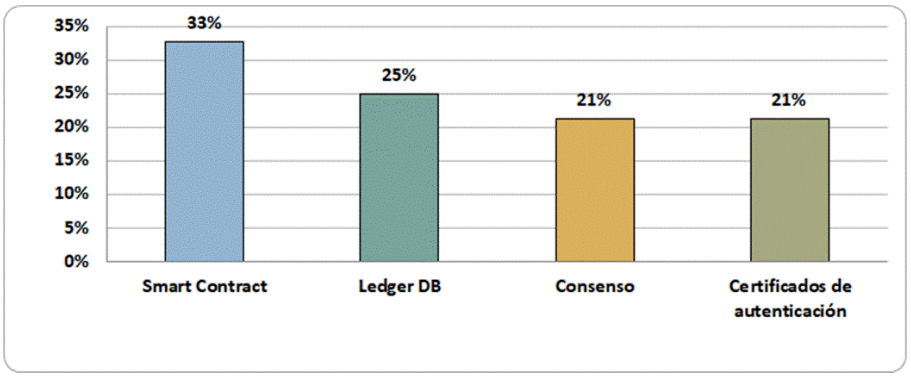


Figura 3. Componentes de Blockchain.

4.1.3 ¿En qué áreas se utiliza Blockchain?

Se hallaron cinco áreas que se utiliza como: Educación en 4%, Energía en 4%, Salud en 13%, Productos en 29% y Finanzas en 50%. Esto quiere decir que, esta tecnología está revolucionando el mercado financiero, cambiando la forma tradicional en que operan los bancos. Se encuentran casos como el Banco de la Reserva de la India que tiene implementaciones en Blockchain, utilizan múltiples lugares distribuidos para compartir, replicar y sincronizar la información. Otro banco privado en la India utiliza Blockchain para transacciones, remesas y financiamiento del comercio. En las entidades financieras se combina los procesos de negociación con la tecnología Blockchain para minimizar las deficiencias, descentralizar las actividades, evitar las manipulaciones, cifrar de forma segura los datos, para obtener un entorno de transacciones más transparente y seguro. Ver figura 4.

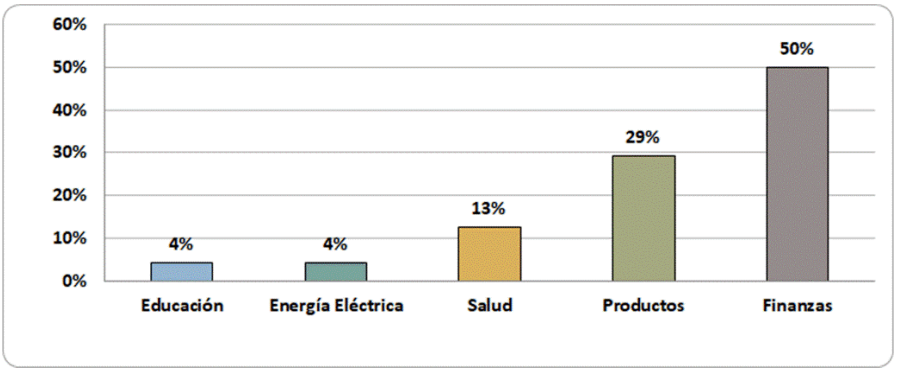


Figura 4. Áreas utilizan Blockchain.

4.1.4 ¿Qué herramientas de software se utilizan?

Se hallaron tres herramientas que se utiliza como: Ethereum en 57%, Solidity en 18% e Hyperledger en 25%. De acuerdo con la lectura, los prototipos en Ethereum son de cadena pública, no se garantiza la privacidad del usuario y no es intervenida por un gobierno; además trabaja con SC que necesitan la criptomoneda ether para su ejecución. Por otra parte, los prototipos en Hyperledger permiten transacciones basadas con mejor o mayor velocidad; aunque la utilización de canales para la privacidad plantea inquietudes sobre la escalabilidad y complejidad de la red cuando se incrementa la cantidad de usuarios. Por otra parte, Solidity mantiene la privacidad y la velocidad, aunque tiene ciertos problemas de resiliencia (M. M. Islam & In, 2023) ver figura 5.

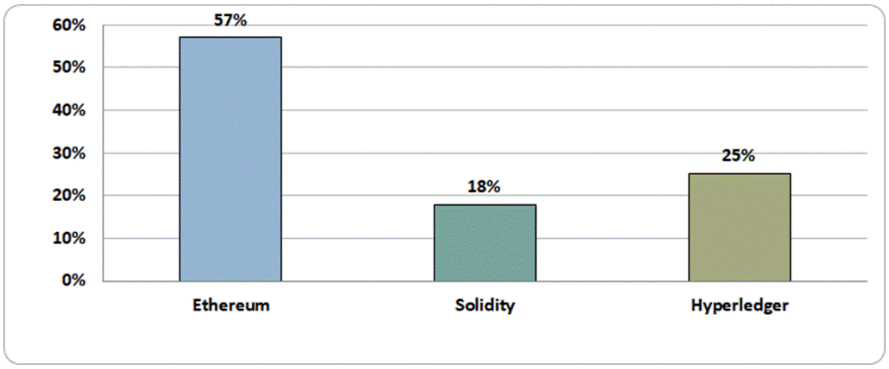


Figura 5. Herramientas de implementación.

4.1.5 ¿Qué clase de diagramas se presentan en los artículos?

Se hallaron cuatro clases de diagramas que se presentaron en los artículos como: Diagramas de Secuencia en 26%, Diagrama de Datos en 17%, Diagrama de Arquitectura en 35%, Algoritmos en 22%. Ver figura 6. Esto quiere decir que, 16 de los 24 artículos presentaron la arquitectura o modelo, en forma general presentan los componentes como participantes, ledger, Smart Contract, certificado de identidad, dispositivos-medios de comunicación, nombre de los nodos, aplicaciones informáticas, herramientas de análisis de datos, entre otros. Los componentes que se presentaron en los diagramas de arquitecturas son útiles para formar o adoptar el nuevo modelo que se propone en esta investigación.

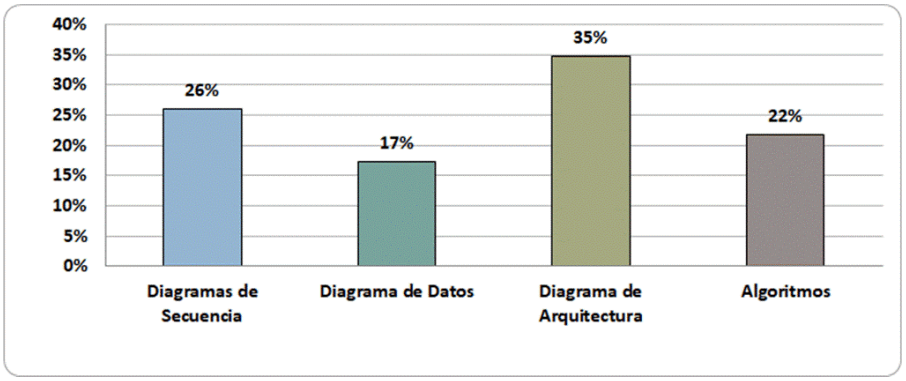


Figura 6. Diagramas.

4.1.6 ¿Qué plataformas se utilizan en los modelos Blockchain?

Se hallaron cuatro plataformas que se diseñaron o implementaron en artículos como: Pública en 52%, Privada en 19%, Consorcio en 19% e Híbrida en 10%. Esto quiere decir que, la mayoría de las arquitecturas diseñaron o implementaron en plataforma pública, estas arquitecturas utilizan herramienta Ethereum que sirve para desarrollar aplicaciones informáticas Blockchain. Las plataformas privadas utilizan la herramienta Hyperledger en sus aplicaciones informáticas. Las plataformas Consorcio o Híbrida utilizan la herramienta Solidity ver figura 7.

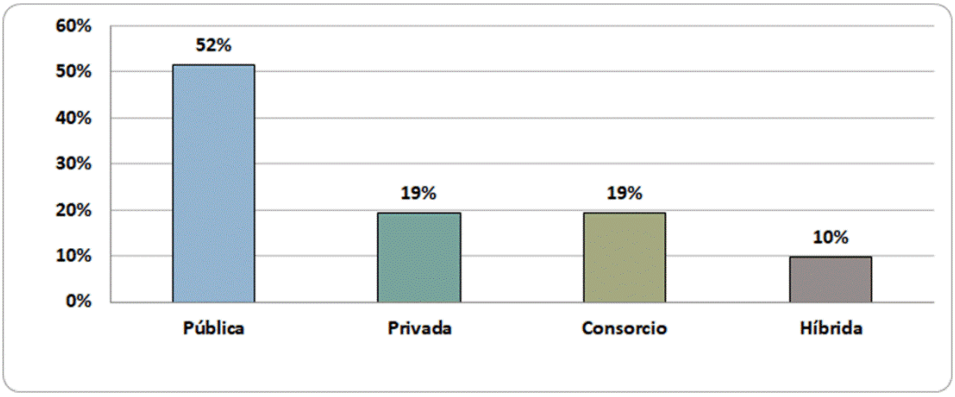


Figura 7. Tipos de plataformas.

4.1.7 ¿Otras tecnologías adicionales se utilizan con Blockchain?

Se hallaron dos tecnologías adicionales que se utilizan en combinación con Blockchain en los artículos como: Internet de las Cosas en 24%, Inteligencia Artificial en 16%, los demás artículos trabajaron solo en Blockchain. Los 6 artículos que utilizaron IoT, al tener un ecosistema IoT mantienen sensores que capturan los datos y los proveen a las aplicaciones que los alimentan como transacciones monetarias para suplir a los productores de datos. Esto es importante en los pagos y mercados de IoT para suministrar las micro-transacciones de los dispositivos IoT

conectados, esta clase de dispositivos generan datos heterogéneos, descentralizados y diversos en su estructura. Aquí, Blockchain supera ciertos problemas en la realización de pagos y mercados IoT como sobresalir la interoperabilidad deficiente, las restricciones de recursos y las debilidades de seguridad y privacidad en las plataformas IoT. Por otra parte, los 4 artículos que utilizaron Inteligencia Artificial mantienen algoritmos como Convolutional Neural Network CNN para entrenar y minimizar alternativas de costos ver figura 8.

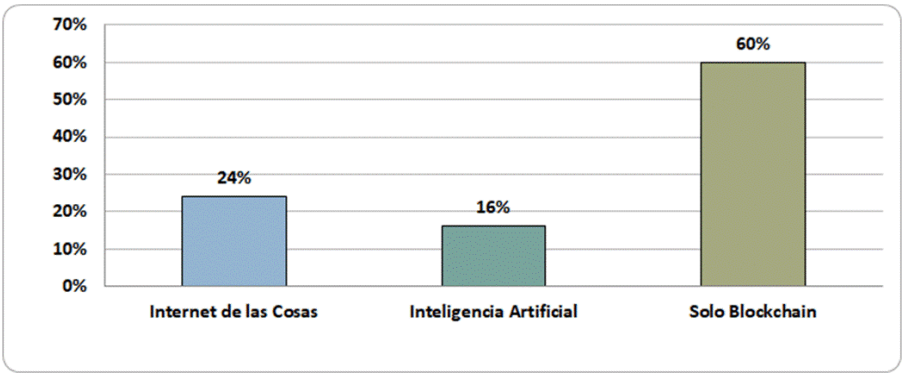


Figura 8. Otras tecnologías.

4.2. Diseñar un modelo distribuido para la seguridad de datos generados en Corresponsales No Bancarias basado en tecnología Blockchain

En esta investigación se propone una solución genérica capaz de adaptarse en otros bancos con infraestructura apropiada. Se presentan componentes y módulos que se visualizan en la Figura 9. El modelo es descentralizado por medio de Blockchain autorizado. Los usuarios de los Corresponsales No Bancarios (CNB) son los clientes de la banca y no clientes. La tecnología Blockchain hace que el modelo sea seguro, transparente y distribuido en las transacciones diarias. El modelo ofrece una interacción segura entre los actores interesados, como Corresponsales No Bancarios, Bancos, Superintendencia de Bancos y Banco Central.

El modelo se propone con las siguientes Operaciones Transaccionales: Obtener Identificación de Uso Único (IUU), consultar saldo, depositar pago, retiro de ahorros, pago de préstamos, pago de agua potable, pago de electricidad, pago de plan celular, pago de teléfono convencional.

Roles funcionales:

- Banco: Es la entidad financiera interesada en participar en el consenso, puede operar o gestionar la cadena de bloques desde un sitio web.

- Entidades de Control: Entidades como la Superintendencia de Bancos, Banco Central del Ecuador y Junta Monetaria, que pueden auditar o revisar las transacciones de la cadena que fueron generadas desde los Corresponsales No Bancarios. Pueden validar las transacciones transmitidas mediante computadoras de alto rendimiento.
- Corresponsales No Bancarios: Son los puntos de generación para las transacciones de los clientes, estos puntos deben ser registrados por el banco en la cadena de bloques.
- Clientes: Personas o empresas que realizan transacciones en los Corresponsales No Bancarios; estos clientes reciben un código de verificación temporal y única para autorizar la transacción.

El modelo consta de cinco secciones: Clientes, Red de Corresponsales No Bancarios, Red de Transmisión, Banco, Entidades de Control.

- Sección Clientes: Se encuentran toda persona o empresa que puede o no ser cliente del banco, es decir clientes bancarizados o no bancarizados. El cliente solicita una transacción, al requerir la transacción entonces el cliente recibe un código llamado Identificación de Único Uso; luego de confirmar la transacción con el IUU el cliente entrega el dinero o recibe el dinero, y recibe el comprobante.
- Sección Red de Corresponsales No Bancarios: Es toda tienda o bazar o cualquier local comercial que tiene acceso a la aplicación bancaria, y puede realizar las transacciones permitidas por el banco. El CNB genera una clave pública, luego solicita el IUU a través de internet, luego que el cliente recibe el IUU, el CNB solicita la generación de la operación transaccional en conjunto con la clave pública y el IUU del cliente. Al recibir una respuesta afirmativa del banco se guarda la transacción con los datos del CNB en la cadena Blockchain.
- Sección Red de Transmisión: Es el medio de transmisión para acceso a internet, puede ser por medio de fibra óptica, vía celular, red privada u otro medio.
- Sección Banco: Es la entidad financiera que tiene los datos del cliente bancario o de la empresa que ofrece los servicios de agua, electricidad, telefonía celular o telefonía fija. El banco tiene su clave privada y la compara con la clave pública del CNB; se valida el usuario del CNB, luego se genera la IUU y se envía al teléfono celular del cliente por medio de un mensaje de texto. Si el CNB solicita la operación transaccional entonces el banco, vuelve a validar la IUU y luego genera la transacción que afecta a los datos. En forma interna, se

adiciona un bloque de transacción a la cadena Blockchain con los datos de la transacción. Si se trata de consultas, pago de préstamos, depósitos en cuenta ahorro y depósitos en cuenta corrientes entonces los valores de dinero se quedan en la cuenta del banco. Si se trata de pago de servicios (pago de agua potable, pago de electricidad, pago de plan celular, pago de teléfono convencional) entonces los valores de dinero se trasladan a la cuenta de la empresa dueña del servicio.

- Sección Entidades de Control: De acuerdo con las leyes de Ecuador, son las entidades que gestionan y disponen lineamientos a los bancos. Estas solo pueden realizar consultas de las transacciones en la cadena Blockchain ver figura 9.

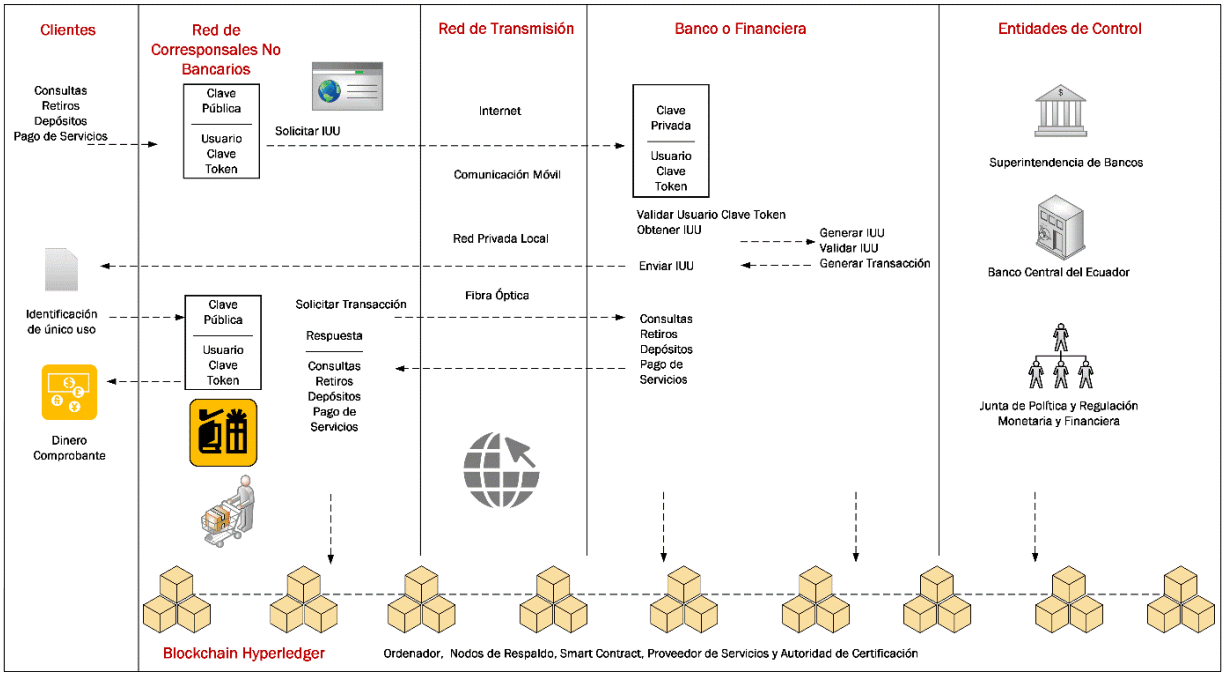


Figura 9. Modelo distribuido.

Características del modelo: Es escalable porque se espera que el sistema de la red Blockchain soporte 1000 conexiones simultáneas o más, en tiempo de ejecución el rendimiento promedio de una transacción debe ser máximo tres segundos, y una tasa de error máxima de 10% de las transacciones por día. A nivel general el rendimiento puede probarse con 100, 500 y 1000 transacciones de usuarios concurrentes, es decir pueden consumir 2000 peticiones en un segundo. Estos parámetros son requisitos mínimos de rendimiento en una aplicación Blockchain.

Suposiciones: Los nodos o Corresponsales No Bancarios ejecutan transacciones computacionales iguales y estables. El bloque de datos es suficiente para contener toda

transacción para su gestión inmediata porque la tasa de transacciones podría ser menor que la cadena privada Hyperledger. Transacciones con tarifa cero. El ancho de banda en la red es apto para el tráfico de datos en relación con Blockchain.

Como herramienta de software se propone utilizar Hyperledger Fabric que mantiene a los interesados del negocio y se encuentran distribuidos geográficamente. Puede gestionar grandes volúmenes de transacciones entre los interesados de la red, además estas transacciones son confiables, inmutables y rastreables dentro de un sentido de confianza. Al momento que los Corresponsales No Bancarios en la red generan una transacción en el ledger de Blockchain, todos los ledger se actualizan en forma simultánea. Dentro de la cadena, se adiciona un nuevo bloque con los datos relacionados al cliente y la transacción que se generan desde el Corresponsal No Bancario. En Hyperledger, se crea un canal que establece una red de comunicación entre los participantes. Además, tiene un Ordenador, Nodos de Respaldo, Smart Contract, Proveedor de Servicios y Autoridad de Certificación. Cada participante tiene credenciales asignadas por un Proveedor de Servicios. La Autoridad de Certificación facilita el acceso administrativo para adicionar bancos, Corresponsales No Bancarios, entidades gubernamentales de control, generar el certificado y las claves públicas-privadas para los participantes, esto mantiene la comunicación de la red en forma segura. Las claves criptográficas las utiliza el Corresponsal No Bancario y el Banco a través de la red para mantener las transacciones cifradas y hacer más confiables todo movimiento. Toda transacción está firmada digitalmente con la clave pública del Corresponsal No Bancario y utilizando la clave privada del Banco.

El Smart Contract se desarrolla dentro de la cadena de bloques, las condiciones y términos del contrato se monitorean en toda la cadena, cada evento y dato vinculado con el contrato se guarda en la cadena. El Smart Contract tiene las siguientes funciones: Validar usuario, obtener IUU, enviar IUU, generar IUU, validar IUU, consultar saldo, depositar pago, retiro de ahorros, pago de préstamos, pago de agua potable, pago de electricidad, pago de plan celular, pago de teléfono convencional.

La transparencia de las transacciones en la primera característica del modelo; el registro de las transacciones en el ledger distribuido hace que sean visibles al banco y entidades de control; el control y seguimiento es una aplicación beneficiosa en las finanzas internacionales por la mala conducta identificada por las autoridades o en la malversación de fondos en crisis financiera.

Es relevante señalar que la transparencia puede entrar en conflicto con otros estándares de los mercados financieros internacionales. Por exigencias de la ley, los bancos están obligados a mantener el sigilo bancario de sus clientes. Otro punto que mantiene el modelo es la integridad de los datos que es la exactitud y coherencia de los datos todo el tiempo. La permanente integridad de los datos mantiene la confidencialidad y la autorización.

4.3. Evaluar el modelo distribuido para la estimación de la viabilidad y aplicabilidad mediante la estrategia Blockchain integrada

Se utilizan indicadores numéricos de la Metodología iBS-BlockchainDD (Labs, 2024) que consiste en tres fases: Análisis de uso, Análisis de naturaleza y viabilidad, Evaluación de potencialidad e interés. Estos indicadores tienen una puntuación entre 1 y 5. La metodología utilizada es una herramienta de evaluación y comprensión teórica sobre el caso de uso en nodos de agencias no corresponsales basado en tecnología Blockchain; aunque no existe el análisis financiero ni económico sobre el diseño. Esta evaluación permite un entendimiento previo sobre el caso bancario, en caso de pretender realizar la implementación a través de Blockchain.

Tabla 2. Artículos seleccionados

Fase	**Valor**
Análisis de uso	
Prueba de existencia	4
Prueba de no existencia	1
Prueba de orden	3
Prueba de identidad	4
Prueba de autoría	5
Análisis de naturaleza y viabilidad	
Requisitos de uso	5
Utiliza un tipo de cadena	5
Utilidad de la aplicación	4
Mantiene integridad	4
Desarrollo del negocio	4
Evaluación de potencialidad e interés	
Justificable	5
Escalable	5
Extrapolable	3
Persistente	5
Desarrollo	0
Aceptable	4

Fuente: Autoría propia.

De acuerdo con la metodología; se consideran puntos críticos el puntaje 0 y 1; se consideran puntos por mejorar el puntaje 2 y 3; se consideran puntos ideales el puntaje 4 y 5.

Puntos críticos: En las Pruebas de No Existencia se destaca que elementos como créditos sin débitos, no existen dentro de la cadena de Corresponsales No Bancarios. El Desarrollo define la implementación total en los corresponsables, tiene calificación cero porque solo se propone el diseño del modelo.

Puntos por mejorar: La Prueba de Orden define las características de procesos secuenciales en la cadena de Corresponsales No Bancarios. El Extrapolable significa que este modelo distribuido pueda ajustarse e implementarse en otros sectores como salud o gobierno.

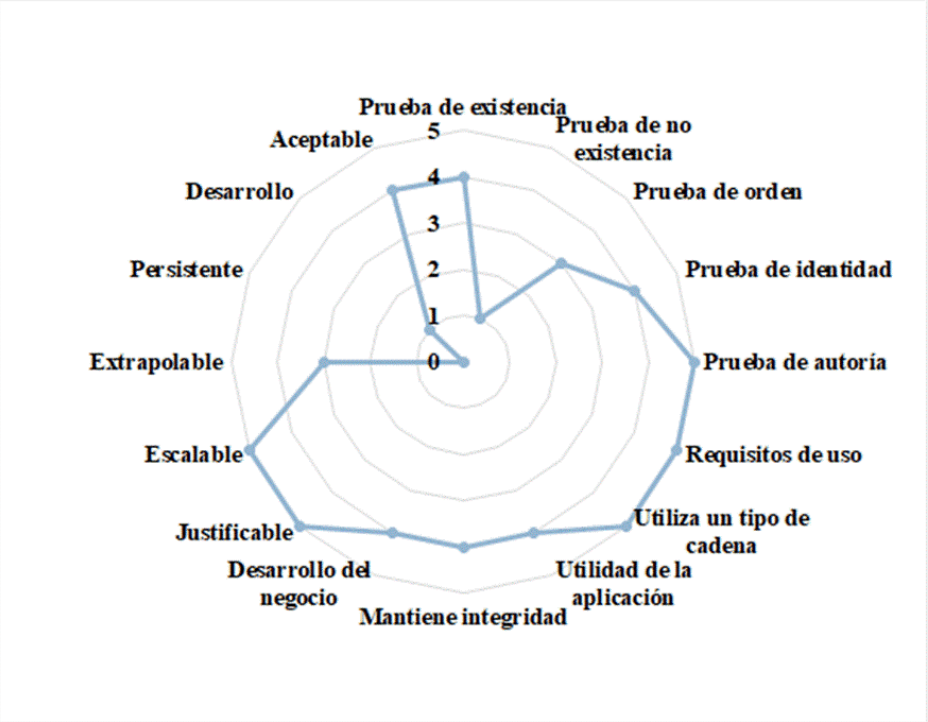


Figura 10. Evaluación teórica.

Puntos ideales: La Prueba de Existencia se refiere al almacenamiento de los datos en bloques con marca de tiempo y secuencia de registro único. La Prueba de Identidad determina la existencia de transacciones o identificación de clientes o proveedores de servicios. La Prueba de Autoría muestra el autor de la transacción bancaria en los nodos o Corresponsales No Bancarios, y que terceros no puedan adicionar datos sin autorización. El Requisito de Uso sobre la cadena de Corresponsales No Bancarios sea fiable y mantenga la autenticidad. Utiliza un tipo de cadena está basada en plataforma privada. Utilidad de la Aplicación hace que la cadena en este tipo de negocio crea valor de seguridad en los corresponsales y clientes. Mantiene la Integridad porque se mantiene durante todo el funcionamiento de la cadena de Corresponsales No Bancarios. Desarrollo del Negocio establece el grado que está respaldado en un negocio

bancario ya establecido. Es Justificable porque este modelo propuesto resuelve los desafíos de seguridad y privacidad en el sector bancario. Es Escalable porque este modelo propuesto puede llegar a más agencias Corresponsales No Bancarios y a más clientes. Es Aceptable porque se utiliza la tecnología Blockchain que es competente en otras áreas ya comprobadas, y esta tecnología se encuentra en desarrollo.

5. DISCUSIÓN

En los componentes de seguridad, la Transparencia e Integridad se igualan en 15 artículos o 63%; la Confiabilidade Integridad se igualan en 11 artículos o 46%; la Disponibilidad y Transparencia se igualan en 12 artículos o 50%; la Trazabilidad y Privacidad se igualan en 8 artículos o 33%. En los componentes de Blockchain que son: Smart Contract, Ledger DB, Consenso y Certificados de autenticación. Solo 7 de los 24 artículos se igualan en los cuatro componentes. 9 de los 24 artículos se igualan en los tres primeros componentes. En las clases de diagramas, los 10 artículos que presentaron Algoritmos también presentaron Diagrama de Arquitectura. Los 12 artículos que presentaron Diagramas de Secuenciase igualan con los artículos que presentaron Diagrama de Arquitectura. Los 8 artículos que presentaron Diagrama de Datos se igualan con los artículos que presentaron Diagramas de Secuencia. Solo un artículo realiza el diseño de una arquitectura basada en Blockchain, Internet de las Cosas e Inteligencia Artificial.

No se modelan los costos operativos ni implementación acerca de esta arquitectura, el diseño tiene propiedades para gestionar pagos desde los Corresponsales No Bancarios para que sean eficientes y confiables. En las plataformas se debe destacar que las herramientas de software, Ethereum se utiliza para plataformas públicas, Hyperledger se utiliza para plataformas privadas.

Se escogió Hyperledger por ser una plataforma privada entre los Corresponsales No Bancarios y el Banco. El modelo propuesto en Hyperledger mantiene la confidencialidad e integridad de las transacciones con la privacidad, y puede tener canales que son subredes privadas de comunicación entre dos o más participantes de la red. Además, las transacciones de la red se ejecutan dentro de un canal, cada Corresponsal No Bancario debe estar autenticado y autorizado para generar transacciones.

El Smart Contract, garantiza el no cambio arbitrario de las funcionalidades, por lo tanto, los comportamientos maliciosos y fraudes financieros, se mitigan en gran medida y se reduce el riesgo para el banco y los clientes.

La viabilidad y aplicabilidad mediante la estrategia Blockchain integrada especifica que, entre los 16 puntos, existen 12 puntos que hace que el modelo sea viable.

6. CONCLUSIÓN

El objetivo general es cubierto por el modelo que se propone basado en Blockchain Hyperledger que gestiona las transacciones en forma fácil y seguro entre los participantes. Permite la comunicación directa por medio de un repositorio compartido y encriptado. Esto minimiza a cero las manipulaciones de datos, además genera transparencia y confianza entre los participantes.

El análisis de 24 artículos científicos que contienen modelos o casos de implementación se utilizaron para adoptar componentes ya probados, los modelos analizados son arquitecturas diseñadas por la comunidad científica. Blockchain es una tecnología que está en continuo crecimiento y pruebas en el área financiera bancaria.

La transparencia, la trazabilidad, la seguridad y la inmutabilidad están garantizadas en el modelo distribuido que se propone en esta investigación gracias a la tecnología Blockchain, y el modelo está diseñado sobre Hyperledger para gestionar las transacciones en forma privada, es decir entre los interesados como los Corresponsales No Bancarios, Bancos y Entidades de Control Ecuatoriano.

Las transacciones generadas desde los Corresponsales No Bancarios se mantienen en la cadena de bloques con una marca de tiempo, los auditores pueden verificar y rastrear las transacciones revisando cualquier nodo en la cadena distribuida. La auditoría mejora la trazabilidad y la transparencia de las transacciones.

REFERENCIAS

Abdelsalam, M., Shokry, M., & Idrees, A. M. (2024). A Proposed Model for Improving the Reliability of Online Exam Results Using Blockchain. *IEEE Access*, *12*(August 2023), 7719–7733. https://doi.org/10.1109/ACCESS.2023.3304995

Agrawal, K., Aggarwal, M., Tanwar, S., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). An Extensive Blockchain Based Applications Survey: Tools, Frameworks, Opportunities, Challenges and Solutions. *IEEE Access*, *10*(October), 116858–116906. https://doi.org/10.1109/ACCESS.2022.3219160

Al-Shaibani, H., Lasla, N., & Abdallah, M. (2020). Consortium Blockchain-Based Decentralized Stock Exchange Platform. *IEEE Access*, *8*, 123711–123725. https://doi.org/10.1109/ACCESS.2020.3005663

Alzhrani, F. E., Saeedi, K. A., & Zhao, L. (2022). A Taxonomy for Characterizing Blockchain Systems. *IEEE Access*, *10*(August), 110568–110589. https://doi.org/10.1109/ACCESS.2022.3214837

Banco de Guayaquil. (2024). *Banco Guayaquil*. https://www.bancoguayaquil.com/banco-del-barrio/

Banco de Loja. (2024). *Banco de Loja*. https://www.bancodeloja.fin.ec/Información/Nuestra-Cobertura/Puntos-de-Pago

Banco del Pacífico. (2024). *Banco del Pacífico*. https://www.bancodelpacifico.com/agencias-y-cajeros

Banco del Pichincha. (2024). *Banco Pichincha*.

Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., & Cao, Y. (2021). A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access*, *9*, 61048–61073. https://doi.org/10.1109/ACCESS.2021.3072849

Chaleenutthawut, Y., Davydov, V., Evdokimov, M., Kasemsuk, S., Kruglik, S., Melnikov, G., & Yanovich, Y. (2024). Loan Portfolio Dataset From MakerDAO Blockchain Project. *IEEE Access*, *12*(January), 24843–24854. https://doi.org/10.1109/ACCESS.2024.3363225

Chang, S. E., & Wang, M. H. (2023). Blockchain-Enabled Fintech Innovation: A Case of Reengineering Stock Trading Services. *IEEE Access*, *11*(November), 137125–137137. https://doi.org/10.1109/ACCESS.2023.3339570

Chen, H., Su, K., & Gao, W. (2022). The Analysis of Blockchain Digital Currency Product Innovation Based on Artificial Immune Algorithm. *IEEE Access*, *10*(December), 132448–132454. https://doi.org/10.1109/ACCESS.2022.3229870

Dashkevich, N., Counsell, S., & Destefanis, G. (2020). Blockchain Application for Central Banks: A Systematic Mapping Study. *IEEE Access*, *8*, 139918–139952. https://doi.org/10.1109/ACCESS.2020.3012295

De Villiers, A., & Cuffe, P. (2020). A Three-Tier Framework for Understanding Disruption Trajectories for Blockchain in the Electricity Industry. *IEEE Access*, *8*, 65670–65682. https://doi.org/10.1109/ACCESS.2020.2983558

Farrell, S. (2019). Blockchain standards in international banking: Understanding standards deviation. *Journal of ICT Standardization*, *7*(3), 209–224. https://doi.org/10.13052/jicts2245-800X.732

Hawashin, D., Mahboobeh, D. A. J., Salah, K., Jayaraman, R., Yaqoob, I., Debe, M., & Ellahham, S. (2021). Blockchain-based management of blood donation. *IEEE Access*, *9*, 163016–163032. https://doi.org/10.1109/ACCESS.2021.3133953

Hu, Y., Manzoor, A., Ekparinya, P., Liyanage, M., Thilakarathna, K., Jourjon, G., & Seneviratne, A. (2021). A Delay-Tolerant payment scheme based on the ethereum blockchain. *IEEE Access*, *7*, 33159–33172. https://doi.org/10.1109/ACCESS.2019.2903271

Islam, M. M., & In, H. P. (2023). A Privacy-Preserving Transparent Central Bank Digital Currency System Based on Consortium Blockchain and Unspent Transaction Outputs. *IEEE Transactions on Services Computing*, *16*(4), 2372–2386. https://doi.org/10.1109/TSC.2022.3226120

Islam, M., Member, G. S., & Islam, K. (2023). A Low-Cost Cross-Border Payment System Based on Auditable Cryptocurrency With Consortium Blockchain : Joint Digital Currency. *IEEE Transactions on Services Computing*, *16*(3), 1616–1629. https://doi.org/10.1109/TSC.2022.3207224

Jabbar, R., Dhib, E., Said, A. Ben, Krichen, M., Fetais, N., Zaidan, E., & Barkaoui, K. (2022). Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review. In *IEEE Access* (Vol. 10). IEEE. https://doi.org/10.1109/ACCESS.2022.3149958

Kimura, L. T., Shiraishi, F. K., Andrade, E. R., Carvalho, T. C. M. B., & Simplicio, M. A. (2024). Amazon Biobank: Assessing the Implementation of a Blockchain-Based Genomic Database. *IEEE Access*, *12*(December 2023), 9632–9647. https://doi.org/10.1109/ACCESS.2024.3354716

Labs, Ic. (2024). *Metodología iBS-BlockchainDD*.

Lee, S., & Kim, S. (2022). Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges. *IEEE Access*, *10*, 2602–2618. https://doi.org/10.1109/ACCESS.2021.3136328

Ma, J., Lin, S., Chen, X. I. N., Sun, H., Chen, Y., Member, G. S., & Wang, H. (2022). A Blockchain-Based Application System for Product Anti-Counterfeiting. *IEEE Access*, *8*, 77642–77652. https://doi.org/10.1109/ACCESS.2020.2972026

Melendrez-Caicedo, G., & Llerena-Izquierdo, J. (2022). Secure Data Model for the Healthcare Industry in Ecuador Using Blockchain Technology. *Smart Innovation, Systems and Technologies*, *252*, 479–489. https://doi.org/10.1007/978-981-16-4126-8_43

Papadis, N., & Tassiulas, L. (2020). Blockchain-Based Payment Channel Networks: Challenges and Recent Advances. *IEEE Access*, *8*, 227596–227609. https://doi.org/10.1109/ACCESS.2020.3046020

Saputhanthri, A., De Alwis, C., & Liyanage, M. (2022). Survey on Blockchain-Based IoT Payment and Marketplaces. *IEEE Access*, *10*(October), 103411–103437. https://doi.org/10.1109/ACCESS.2022.3208688

Syed, T. A., Siddique, M. S., Nadeem, A., Alzahrani, A., Jan, S., & Khattak, M. A. K. (2020). A Novel Blockchain-Based Framework for Vehicle Life Cycle Tracking: An End-to-End Solution. *IEEE Access*, *8*, 111042–111063. https://doi.org/10.1109/ACCESS.2020.3002170

Touloupou, M., Themistocleous, M., Iosif, E., & Christodoulou, K. (2022). A Systematic Literature Review Toward a Blockchain Benchmarking Framework. *IEEE Access*, *10*(July), 70630–70644. https://doi.org/10.1109/ACCESS.2022.3188123

Tran, Q. N., Turnbull, B. P., Wu, H., de Silva, A. J. S., Kormusheva, K., & Hu, J. (2021). A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture. *IEEE Open Journal of the Computer Society*, *2*(January), 72–84. https://doi.org/10.1109/OJCS.2021.3053032

Youn, S., & Cho, H. C. (2021). Blockchain technology in finance industry. *Transactions of the Korean Institute of Electrical Engineers*, *68*(12), 1601–1606. https://doi.org/10.5370/KIEE.2019.68.11.1601

Zerega-Prado, J., & Llerena-Izquierdo, J. (2022). Arquitectura de consolidación de la información para seguros de la salud mediante Big Data. *Memoria Investigaciones En Ingeniería*, *0*(23 SE-Artículos). https://doi.org/10.36561/ING.23.3

Zhang, X., & Ling, L. (2023). A Review of Blockchain Solutions in Supply Chain Traceability. *Tsinghua Science and Technology*, *28*(3), 500–510. https://doi.org/10.26599/TST.2022.9010030

Zhao, G., Dong, J., Liu, M., & Zhai, K. (2022). Evolutionary game of banks and enterprises in digital supply chain finance driven by blockchain. *Proceedings of the 34th Chinese Control and Decision Conference, CCDC 2022*, 5397–5402. https://doi.org/10.1109/CCDC55256.2022.10033844