ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M.
Volume 3, Issue no. 2, DOI 10.18502/espoch.v4i1.15825
Production and Hosting by Knowledge E

Research Article

Proposal for the Transaction Model Based on Blockchain Technology for Financial Operations

Propuesta del modelo de transacciones basado en tecnología Blockchain para las operaciones financieras

Paul del Aguila Caute*, Jhon Villacriz Moran

UNTELS, Facultad de Ingeniería y Gestión, Lima, Lima, Perú

ORCID
Paul del Aguila Caute: https://orcid.org/0000-0003-0966-8843

INDEXACIÓN II CONGRESO INTERNACIONAL DE CIENCIA Y TECNOLOGIA MORONA SANTIAGO CICTMS 2021

Corresponding Author: Paul del Aguila Caute

Published: 18 April 2024

Production and Hosting by Knowledge E

Abstract

There is a need to take measures against financial fraud in banking institutions since it annually generates million-dollar losses in the banking sector and even limits the economy of a country. Although there are methods to avoid these problems, the most manageable is a centralized system where large volumes are processed, which means that they have serious performance and security limitations, making it easy for cybercriminals to attack a single target. Therefore, the objective is to identify the models of Blockchain technology as a measure to reduce bank fraud and propose a new transaction model for financial operations.

The methodology used was the literature review where a total of 200 potential studies were obtained, of which 30 were selected for writing this article. The result of this research is the proposal of a model for financial transactions using Blockchain technology.

Keywords: *blockchain, transactions, security, privacy, finance.*

Resumen

Existe la necesidad de tomar medidas contra el fraude financiero en las instituciones bancarias ya que genera pérdidas de miles de millones de dólares anuales en el sector bancario e incluso limita la economía de un país, aunque es cierto que existen métodos para evitar estos problemas, la mayoría gestiona un sistema centralizado en el que se procesan grandes volúmenes, lo que hace que tengan serias limitaciones de rendimiento y seguridad, lo que facilita que los delincuentes informáticos ataquen a un único objetivo. Por ello, el objetivo es identificar los modelos de la tecnología Blockchain como medida para reducir el fraude bancario y proponer un nuevo modelo de transacción para las operaciones financieras. La metodología usada fue la revisión de la literatura. En la revisión de los artículos se obtuvo un total de 200 estudios potenciales, de los cuales se seleccionaron 30 para la redacción de este artículo. El resultado de esta investigación es la propuesta de un modelo para transacciones financieras utilizando la tecnología Blockchain.

Palabras Clave: *blockchain, transacciones, seguridad, privacidad, finanzas.*

1. Introducción

En la literatura revisada se puede observar como el interés por la tecnología Blockchain es cada vez mayor, siendo aplicado en diversos sectores interesados en proteger sus datos más valiosos, incluyendo el sector financiero, en este sentido Kashyap & Saurap afirman que las una de las principales causas que hacen elevar el grado de desconfianza por parte de los depositantes de los bancos, entre ellas es que no tienen suficiente información, lo que les dificulta protegerse (1).

Según Corredor Higuera & Díaz Guzmán afirman que en los mercados financieros Latinoamericanos significa una limitante para el crecimiento económico (2). Así mismo Aslan indica que las pérdidas financieras por fraudes, Latinoamérica es afectado con más de USD 150.000 en el sector de servicios financieros (3).

En el desarrollo de nuestra investigación nos centraremos en proponer un modelo de transacciones basado en Blockchain para las transacciones financieras, dado que casi todos los sistemas bancarios se basan en una base de datos centralizada, son más propensos a los ataques de penetración, que pueden comprometer la información confidencial de los clientes del banco. Además de los servicios prestados por el banco, el cliente tiene que pagar los gastos generales de la transacción. Por otro lado, el banco tiene que registrar y mantener todos los detalles transaccionales de cada cliente, lo que generalmente es masivo en términos de datos. La tecnología Blockchain es la solución a estos problemas del actual sistema bancario tradicional.

2. Materiales y Métodos

Para esta investigación se utilizó la metodología de revisión de literatura propuesta por Wong (4), esta metodología está determinada por 3 fases:

Planificación de la revisión

Desarrollo de la revisión

Resultados de la revisión

2.1. Planificación de la revisión

Para esta fase se elaboran las preguntas para investigación. Para esta investigación las preguntas que se utilizaron son las siguientes:

Q1: ¿Qué modelos de Blockchain permiten reducir los fraudes bancarios en las transacciones financieras?

Q2: ¿Qué modelos de Blockchain aumentan la privacidad de los datos de los clientes en las transacciones financieras?

Q3: ¿Qué modelo de Blockchain permite aumentar la velocidad de las transacciones financieras?

Se utilizaron principalmente las bases de datos de ScienceDirect, IEEE y Scopus.

2.2. Desarrollo de la revisión

La literatura encontrada en la búsqueda fue sometida a los criterios de selección previamente mencionados en el paso anterior. Para su elección fue necesaria realizar una revisión previa para determinar si su contenido es relevante para la investigación. En la Figura 1 se muestra el proceso de desarrollo realizado.

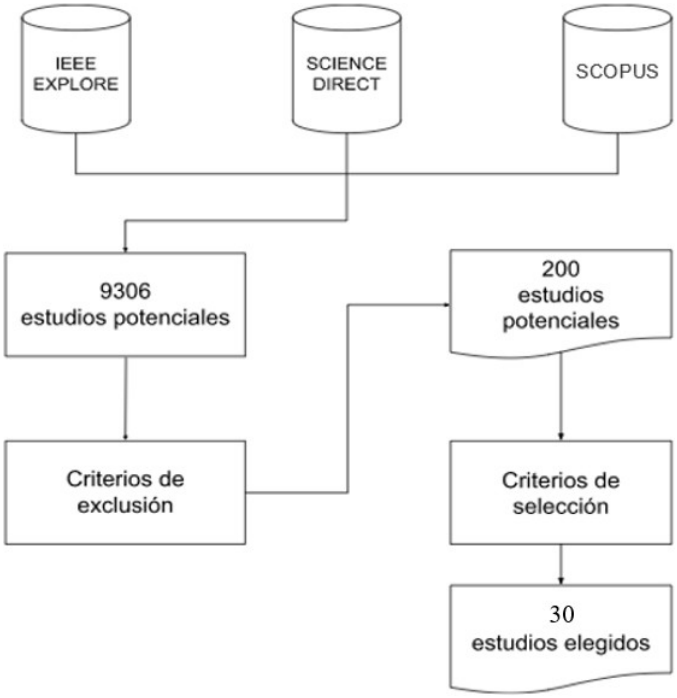

Figura 1

Proceso de selección de artículos.

2.3. Resultados de la revisión

Los resultados obtenidos por la búsqueda de información relevante para la investigación se obtuvieron en

estudios relevantes de los cuales se seleccionaron 40. En la Tabla 1 se muestra la cantidad de estudios obtenidos de las bases de datos.

Tabla 1

Cantidad de estudios.

Fuente	Estudios potenciales elegibles	Estudios elegidos
IEEE Explore	2306	13
Science Direct	6858	8
Scopus	142	9
Total	9306	30

3. Desarrollo y Discusión

Modelos de sistema de transacciones basado en Blockchain que reducen fraudes bancarios:

En la investigación desarrollada por Wang & Kogan (5), los autores proponen un modelo de sistema de transacciones basado en Blockchain usando el cifrado homomórfico, integran la prueba de conocimiento cero para ocultar los detalles de las operaciones y de esta forma proteger la privacidad del usuario, concluyen que mediante el uso de algoritmos criptográficos, Blockchain puede garantizar la integridad de los datos pudiendo aplicarse en la auditoría de control continuo y prevención del fraude.

Según Sangwan (6) en su investigación desarrollan un modelo usando Iroha en un sistema de transacciones basado en Blockchain. Iroha se instaló y configuró en un entorno de prueba utilizando contenedores Docker para configurar varias máquinas virtuales que ejecutaban Iroha en la misma red concluyen que los sistemas que respaldan las transacciones financieras a escala empresarial deben poder manejar grandes volúmenes de transacciones de manera segura y al mismo tiempo mantener un alto nivel de disponibilidad operativa.

Zheng (7) en su investigación desarrollada construyen un sistema basado en Blockchain que proporciona mayor anonimato al usuario, para su construcción hacen uso de la firma grupal y la prueba de conocimiento cero, concluye que su sistema satisface las propiedades de seguridad de protocolo, privacidad de transacciones y trazabilidad de identidad, lo que lo hace adecuado para transacciones de público a público.

Zhang (8) propone un modelo híbrido para moneda digital del banco central basado en Blockchain con una red de modularidad para CBDC a través de diferentes nodos,

se menciona que el análisis y los resultados experimentales muestran que la seguridad del modelo

está garantizada por el esquema de almacenamiento y el mecanismo de consenso.

En el artículo desarrollado por Balagolla (9)los autores desarrollan un modelo de transacciones con tarjeta de crédito basado en Blockchain. En este sistema el consumidor implementa el contrato inteligente, luego al banquero inicia el contrato inteligente y por último los datos de la tarjeta se cifran, concluyen que el sistema propuesto ayudará a las entidades a detectar fraudes antes de que se agraven.

En el artículo desarrollado por Pravin

(10) los autores proponen un sistema que reemplaza la base de datos centralizada con una base de datos descentralizada que distribuye los datos a lo largo de la cadena. En este nuevo sistema será el banco el único que podrá crear nuevos bloques en la cadena, de esta manera será el banco el que verificará, validará y registrará las transacciones.

El modelo propuesto por Lu (11) llamado (BARS) está basado en Blockchain y establece un modelo de confianza para preservar la privacidad. En este modelo cada entidad genera un par de claves públicas y privadas, cuando el cliente ingresa a la red se utiliza un canal seguro para enviar su clave pública para probar su identidad

legal. Las RSU verificarán todas las transacciones de revocación, eliminarán las claves públicas vencidas e insertarán las claves públicas revocadas.

Canillas (12) muestra un modelo de transacciones digitales llamado GraphSif para detectar fraudes en las transacciones financieras. Como se observa en la figura 2, los histogramas se agrupan utilizando k-means y se envían a un mapa autoorganizado. El histograma (conjunto de transacciones histórica) correspondiente a la transacción probada se compara con el modelo y se calcula su similitud con los otros histogramas de su grupo.

Según Weng (13) en su investigación, los autores mencionan que su modelo llamado DeepChain garantiza la privacidad de los datos de cada participante y brinda auditabilidad para todo el proceso de capacitación. Implementan un prototipo de DeepChain y realizan experimentos en un conjunto de datos reales para diferentes configuraciones, y los resultados muestran que DeepChain es prometedora.

En el artículo desarrollado por Ma (14) se menciona un nuevo modelo de gestión de la privacidad de datos basado en blockchain usando la teoría Nudge, que reduce la operación manual y la transformación masiva del sistema. Es necesario construir los servidores locales de blockchain que se comunican en la red bancaria, al mismo tiempo utiliza el sistema de gestión de informacion del cliente empresarial, que se utiliza para

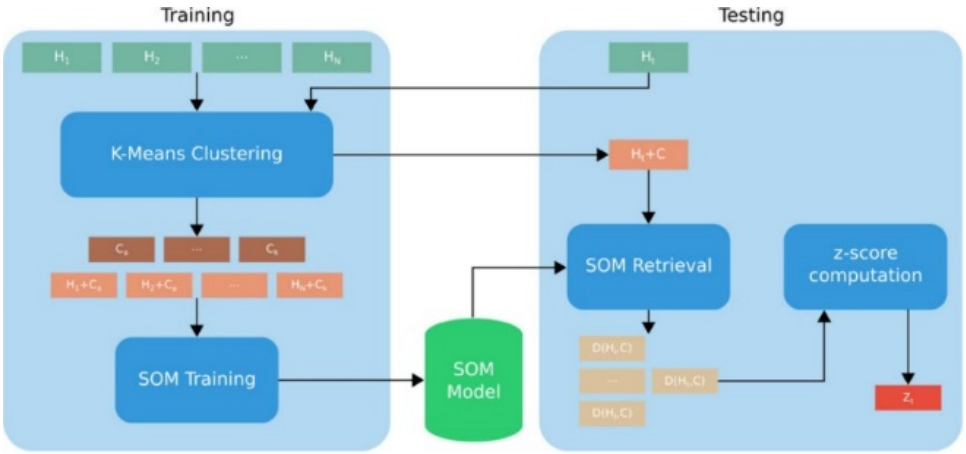

Figura 2

Modelo GraphSif.

guardar la información unificada del cliente del banco, para almacenar la información del cliente fuera de la cadena, para satisfacer las necesidades diarias del banco.

Modelos de sistema de transacciones basado en Blockchain que aumentan la privacidad de los datos de los clientes: En el artículo de Dong (15) los autores presentan un modelo de sistema de identidad auto-soberana basado en blockchain para la banca abierta, como se observa en la figura 3 el modelo contiene 4 capas para mantener los datos de los clientes de forma privada, haciendo uso de la blockchain de Ethereum para almacenar los datos, concluyen que el modelo de sistema de identidad auto-soberana es un modelo actualizado y complejo, que resuelve el problema de privacidad en el intercambio de datos de los clientes.

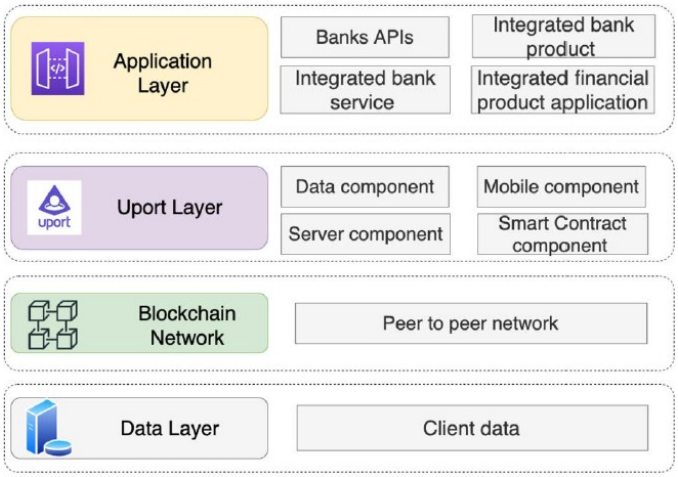

Figura 3

Modelo de identidad auto-soberana.

De acuerdo a los autores de este artículo Sun (16), se propone un modelo de moneda digital para un banco central basado en tecnología blockchain de permisos.

El modelo propuesto hace uso de la arquitectura multi-blockchain y ChainID para mejorar la escalabilidad del modelo y procesar los pagos más rápidamente, concluyen que de esta forma el banco central puede evitar problemas de doble gasto y proteger la privacidad del usuario.

Según Kosba (17) en su estudio presentan Hawk, un sistema de contratos inteligentes que no almacena las transacciones financieras en la blockchain y preserva la privacidad transaccional de la vista del público. Su modelo cuenta con una parte privada, que está destinada a proteger los datos de los participantes, y una parte pública que no toca los datos privados ni dinero. Concluyen que este sistema ofrece

garantías de seguridad que abarcan dos aspectos, privacidad en la cadena y seguridad contractual.

El modelo propuesto por Su (18) presenta una solución segura de intercambio de datos basada en la tecnología blockchain con tecnología de reencriptación de proxy. La solución consiste en un modelo de intercambio de datos y un protocolo de intercambio de datos. En primer lugar, utilizando el almacenamiento distribuido, la gestión descentralizada y las características de no manipulación de blockchain, diseñan un modelo de intercambio de seguridad de datos. El modelo establece estrategias de control de acceso en la plataforma blockchain, y utiliza la plataforma blockchain y las bases de datos distribuidas para almacenar datos cifrados juntos para evitar que los datos confidenciales sean manipulados y filtrados.

En su estudio Norvill (19) proponen un modelo de sistema de transacciones haciendo uso de Blockchain diseñado para mejorar la seguridad y la privacidad tanto de los bancos como de sus clientes, los bancos involucrados tienen interacciones internas y externas basadas en API para cada contenedor y el sistema interno del banco.

Du (20) en su investigación, los autores proponen un nuevo modelo de uso de

cifrado homomórfico basado en Blockchain que resuelve el problema de falta de confianza entre los participantes de la cadena de suministro, reduce costos y mejora los servicios financieros.

Los autores de este artículo Li (21) en su modelo propuesto para sistemas basados en Blockchain utilizan una distribución gaussiana bimodal, el muestreo de rechazo y otras tecnologías para mejorar la seguridad y eficiencia, evitando así la falsificación de los datos. En la investigación desarrollada por Singh (22) los autores proponen un nuevo modelo de seguridad y preservación de la privacidad de los datos en blockchain para un sistema de transacciones. Empieza usando un protocolo de compromiso EC

y NI-Schnorr (autenticación anónima) para preservar de privacidad de los datos y la identidad del remitente, si el verificador valida las firmas del remitente entonces se acepta la solicitud de datos y publicación en la cadena de bloques del receptor, si el receptor desea abrir datos comprometidos, abrirá el compromiso y tiendas en la nube privada.

En el artículo desarrollado por Ma (23) se propone el modelo de intercambio de datos basado en Blockchain, este modelo propuesto

divide los datos en datos públicos que se pueden compartir en texto sin formato y datos privados que deben ser confidenciales, combina la tecnología actual de protección de la privacidad. El esquema IoVChain realizará una serie de procesamientos antes de que los datos se escriban en el bloque, incluida la distribución de claves entre los nodos, la autenticación de identidad, los datos de cifrado homomórfico, la prueba de conocimiento cero, etc.

Xiao (24) en su investigación propone el modelo de un esquema de combinación con un protocolo de firma descentralizado, que no depende de un tercero ni requiere una tarifa de transacción, utiliza un proceso de negociación para garantizar los detalles de la transacción, que es monitoreado por los participantes.

Modelos de sistema de transacciones basado en Blockchain que aumenta la velocidad de las transacciones financieras.

Ye (25) Expone su modelo de sistema de transferencia de fondos de pago transfronterizo basado en Blockchain aplicado en “Oversea-Chinese Banking Corporation”. Este nuevo sistema se desarrolla en base al sistema de pago electrónico MEPS, el modelo es efectivo cuando se necesita transferir

cantidades de dinero entre diferentes países, transformando de esta manera dinero físico en dinero digital.

En el estudio de Kotilevets (26) se presenta la implementación de un modelo de gráfico acíclico dirigido en Blockchain, esto les permitió poder ejecutar cadenas paralelas pudiendo ejecutar simultáneamente diferentes tipos de transacciones en diferentes cadenas. Los autores concluyen que esta nueva estructura permite procesar las transacciones mucho más rápido, procesando hasta 10000 transacciones por segundo, esto significa operaciones casi instantáneas para los usuarios y comisiones significativamente más bajas.

En Bagrecha (27) se muestra un modelo de sistema de transacciones basado en blockchain que se puede aplicar en el sector bancario. En la figura 4 se observa que el sistema cuenta con múltiples nodos de usuario y nodos de verificación. Los nodos

de verificación son responsables de las tareas autorizadas por los clientes. Los nodos de usuario sirven para iniciar una nueva transacción, ver el historial de la cuenta, etc.

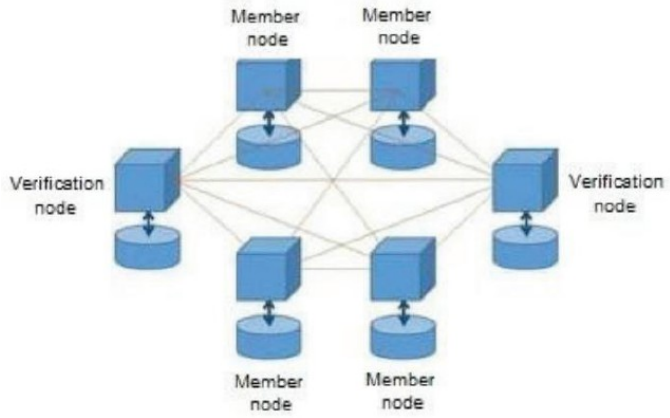

Figura 4

Modelo del sistema con múltiples nodos.

En la investigación desarrollada por Zhang (28) proponen un modelo de optimización para la colocación de transacciones en fragmentos de blockchain. Según el análisis de tiempo y un gráfico de flujo de transacciones, se calcula la aptitud para decidir qué fragmento es el más adecuado para realizar una transacción.

Los autores Rouhani & Detienen, (29) diseñan un modelo de trabajo de extremo a extremo para la confianza de datos utilizando Blockchain, se modela la confianza para los conjuntos de datos de entrada, se calcula su valor de confianza a través de una aplicación basada en blockchain, este valor se usa para confirmar solo datos confiables. Una vez registrados los datos, el propietario puede aceptar solicitudes de acceso a estos datos, usando blockchain, todas las transacciones se aplican automáticamente y no hay terceros involucrados.

Los autores Alharby & van Moorsel (30) presentan su modelo basado en

Blockchain llamado BlockSim. Los resultados de la simulación demuestran que el retraso del bloque podría reducir significativamente el rendimiento, especialmente cuando el intervalo del bloque es pequeño.Por lo tanto, cuanto mayor sea el tamaño del bloque, más tiempo se requerirá para transmitir y verificar el bloque.

Jiang (31) proponen un nuevo modelo de sistema blockchain llamado ParBlockchain para dar solución a transacciones conflictivas mejorando así su rendimiento en cargas de trabajo. Los autores emplean el paradigma orden-ejecución que difieren principalmente en sus rutinas de ordenación, sólo un subconjunto de nodos participa en el protocolo de consenso y segundo, el líder se cambia después de la construcción

de cada bloque, como resultado de las pruebas realizadas el rendimiento de las transacciones se vio menos afectadas.

En el artículo desarrollado por Chen (32) en el modelo de sistema PEEP realizado por los autores proponen una estrategia de confirmación diferida para una mejor utilización de los recursos del sistema, lo que genera un flujo de trabajo sin bloqueos.

El modelo propuesto por Chen (33), llamado SChain, en el cual logran demostrar que simultaneidad intrabloque no solo aprovecha el procesador multinúcleo en un solo par, sino que también aprovecha la capacidad de múltiples pares, lo que permite el procesamiento simultáneo en múltiples bloques. Así, cada organización puede dedicar más ejecutores a pedido para aumentar el paralelismo y procesamiento de ejecución.

Según Tsoulias (34) proponen un modelo de aplicación descentralizado en Python, donde los datos de la cadena de bloques se almacenan en una base de datos de gráficos Neo4j. Muestran como un gráfico distribuido puede ayudar a las operaciones de los protocolos, mejorar su seguridad y facilitar la aplicación de métodos analíticos a la información almacenada a través de consultas dependientes de la ruta.

Para la propuesta del modelo, en el cual se tomaron de referencia los modelos analizados en el marco teórico, presenta el siguiente funcionamiento, tal como se puede observar en la figura 5.

En nuestro modelo la institución financiera actualizará la información en su base de datos que a la vez va extraer la información de las múltiples operaciones que sean realizadas, en nuestra sección de operaciones

financieras, tendremos nuestro cifrado homomórfico y la prueba de conocimiento cero integrado a esta, que servirá para proteger los datos y evitar potenciales fraudes financieros, por último, se incluye un grafo acíclico que nos permite aumentar la velocidad de las operaciones financieras. Una vez terminado el proceso de la operación se añadirá la transacción a nuestra Blockchain haciendo uso de contratos inteligentes y guardando la información generada en los múltiples nodos que podrá ser requerido por los usuarios que lo necesiten.

4. Conclusiones

Este artículo revisa la literatura sobre modelos de transacciones financieras que utilizan la tecnología Blockchain de 3 fuentes principales (IEE Explorer, Science Direct y Scopus) podemos destacar que, de 200 artículos, 30 fueron seleccionados debido a la información relacionada con el tema de investigación.

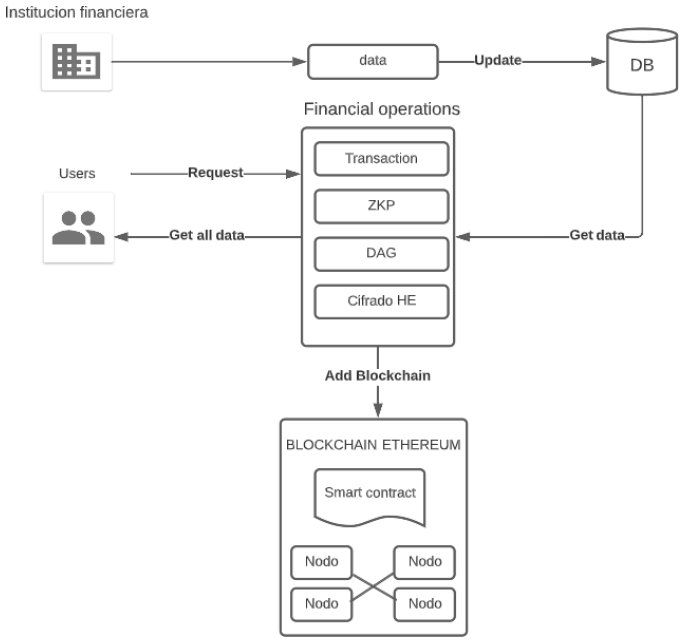

Figura 5

Modelo conceptual propuesto.

Del análisis de los resultados encontrados como se muestra en la figura n. los principales tipos modelos de que más destaca para la reducción de fraudes representa el 32.5%, continua con los modelos de privacidad de datos que representa el 40% y del mismo modo, el tercer tipo de modelo que aumenta la velocidad en las transacciones con un 27.5%.

Teniendo en cuenta los tipos de modelos que más sobresalen, el modelo de Blockchain híbrido resulta ser uno de los mejores en tema de reducción de fraudes bancarios y en aumentar la velocidad de las transacciones, mientras que el modelo multi-Blockchain resultó ser más utilizado en temas de protección de los datos de los clientes, se puede concluir que el uso de la tecnología Blockchain en las transacciones financieras brinda mayor ventaja en la privacidad de datos permitiendo a los instituciones bancarias tener cada vez más seguridad y transparencia sin la participación de un tercero de confianza, de esta manera facilita rastrear e identificar los registros de las transacciones bancarias, aumentar la velocidad en las transacciones y reducir las pérdidas financieras.

References

[1] Kashyap R, Saurav V. Blockchain technology: Road to transform the Indian banking sector. Materials Today: Proceedings [Internet]. 2021;(xxxx):2–5. Available from:

https://doi.org/10.1016/j.matpr.2021.02. 774

[2] Corredor Higuera JA, Díaz Guzmán D. Blockchain y mercados financieros: aspectos generales del impacto regulatorio de la aplicación de la tecnología blockchain en los mercados de crédito de América Latina. Derecho PUCP. 2018; 405–439 p. Available from: https://doi.org/10.18800/derechopucp.2 01802.013

[3] Aslan, L. Financial statement fraud in the Turkish financial services sector. Istanbul Business Research. 2021;0(0):0–0. Available from: https://doi.org/10.26650/ibr.2021.50.844 527

[4] Wong LR, Mauricio D, Rodriguez GD. A systematic literature review about software requirements elicitation. Journal of Engineering Science and Technology. 2017; 12(2):296–317.

[5] Wang Y, Kogan A. Designing confidentiality-preserving Blockchain-based transaction processing systems. International Journal of Accounting Information Systems. 2018;30(xxxx):1–18. Available from: 10.1016/j.accinf.2018.06.001.

[6] Sangwan RS, Kassab M, Capitolo C. Architectural considerations for blockchain based systems for financial transactions. Procedia Computer Science. 2020;168(2018):265–271. Available from: 10.1016/j.procs.2020.02.252.

[7] Zheng H, Wu Q, Xie J, Guan Z, Qin B, Gu Z. An organization-friendly blockchain system. Computer Security. 2019; 88:101598. Available from: c10.1016/j.cose.2019.101598v

[8] Zhang J, Tian R, Cao Y, Yuan X, Yu Z, Yan X, et al. A Hybrid model for central bank digital currency based on blockchain. IEEE Access. 2021;9:53589–53601. Available from: 10.1109/ACCESS.2021.3071033

[9] Balagolla EMSW, Fernando WPC, Rathnayake RMNS, Wijesekera MJMRP, Senarathne AN, Abeywardhana KY. Credit card fraud prevention using Blockchain. 2021 6th International Conference on Convergence in Technology I2CT 2021. 2021;1–8. Available from: 10.1109/I2CT51068.2021.9418192.

[10] Pravin NP, Anil KP, Sunil SM, Kundlik MS, Suhas PA. Block chain technology for protecting the banking transaction without using tokens. Proc 2nd International Conference on Inventive Research in Computing Applications ICIRCA 2020. 2020;801–807. Available from: 10.1109/ICIRCA48905.2020.9183333.

[11] Lu Z, Liu W, Wang Q, Qu G, Liu Z. A privacy-preserving trust model based on blockchain for VANETs. IEEE Access. 2018; 6: 45655–45664. Available from: 10.1109/ACCESS.2018.2864189

[12] Canillas R, Hasan O, Sarrat L, Brunie L. GraphSIF: Analyzing flow of payments in a Business-to-Business network to detect supplier impersonation. Applied Network Science. 2020;5(1):1–32. Available from: 10.1007/s41109-020-00283-1.

[13] Weng J, Weng J, Zhang J, Li M, Zhang Y, Luo W. DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive. IEEE Transactions on Dependable and Secure Computing. 2019; PP (8):1–1. Available from: 10.1109/tdsc.2019.2952332.

[14] Ma S, Guo C, Wang H, Xiao H, Xu B, Dai HN, et al. Nudging data privacy management of open banking based on blockchain. Proc - 2018 15th International Symposium Pervasive System Algorithms Networks, I-SPAN 2018. 2019;72–79. Available from: 10.1109/I-SPAN.2018.00021

[15] Dong C, Wang Z, Chen S, Xiang Y. BBM: A blockchain-based model for open banking via self-sovereign identity [Internet]. Vol. 12404 LNCS, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer International Publishing; 2020. 61–75 p. Available from: http://dx.doi.org/10.1007/978-3-030-59 638-5_5

[16] Sun H, Mao H, Bai X, Chen Z, Hu K, Yu W. Multi-blockchain model for central bank digital currency. Parallel and Distributed Computing, Applications and Technologies. 2018;2017-Decem:360–367. Available from: 10.1109/PDCAT.2017.00066.

[17] Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. Proc - 2016 IEEE Symposium on Security and Privacy, SP 2016. 2016;839–858. Available from: 10.1109/SP.2016.55

[18] Su Z, Wang H, Xin H. A financial data security sharing solution based on blockchain technology and proxy re-encryption technology. IEEE Access. 2020;5–8. Available from: 10.1109/IICSPI51290.2020.9332363

[19] Norvill R, Cassanges C, Shbair W, Hilger J, Cullen A, State R. A security and privacy focused KYC data sharing platform. BSCI 2020 - Proc 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, Co-located with AsiaCCS 2020. 2020;151–60. Available from: 10.1145/3384943.3409431

[20] Chen Z, Qi X, Du X, Zhang Z, Jin C. PEEP: A parallel execution engine for permissioned blockchain systems. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). LNCS April 2021;12683:341–357. Available from: 0.1109/TEM.2020.2971858

[21] Li C, Tian Y, Chen X, Li J. An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems. Information Sciences (Ny) [Internet]. 2021;546:253–264. Available from: https://doi.org/10.1016/j.ins.2020.08.03 2

[22] Singh K, Heulot N, Hamida E Ben. Towards anonymous, unlinkable, and confidential transactions in blockchain. Proc - IEEE 2018 International Congress on Cybermatics 2018 IEEE International Conference on Internet of Things, Green Computing Commun Cyber, Physical Social Computing Smart Data, Blockchain, Computer Science and Information Technology iThings/Gree. 2018;(May):1642–1649. Available from: 10.1109/Cybermatics_2018.2018.00274

[23] Ma Z, Wang L, Zhao W Blockchain-driven trusted data sharing with privacy protection in IoT Sensor Network. IEEE Sensors Journal. 2021;21(22):25472–25479. Available from: 10.1109/JSEN.2020.3046752

[24] Xiao R, Ren W, Zhu T, Choo KKR. A mixing scheme using a decentralized signature protocol for privacy protection in Bitcoin Blockchain. IEEE Transactions on Dependable and Secure Computing. 2021;18(4):1793–1803. Available from: 10.1109/TDSC.2019.2938953

[25] Ye S, Zhu Y, Lu E. The innovation of retail banks in the cross-border payment fund transfer system: Take OCBC as an example. Mod Econ. 2019;10(05):1479–1486. Available from: 10.4236/me.2019.105098.

[26] Kotilevets ID, Ivanova IA. Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions. IFAC-PapersOnLine. 2018;51(30):693–696. Available from: 10.1016/j.ifacol.2018.11.213

[27] Bagrecha NR, Mustafa Polishwala I, Mehrotra PA, Sharma R, Thakare BS. Decentralized blockchain technology: Application in banking sector. 2020 International Conference for Emerging Technology INCET 2020. 2020;1–5. Available from: 10.1109/INCET49848.2020.9154115.

[28] Zhang PY, Wang LC, Li CX, Zhou MC. An optimization model for transaction placement in blockchain shards. IFAC-PapersOnLine [Internet]. 2020;53(5):374–378. Available from: https://doi.org/10.1016/j.ifacol.2021.04. 115

[29] Rouhani S, Deters R. Data trust framework using blockchain technology and adaptive transaction validation. IEEE Access. 2021;9:90379–90391. Available from: 10.1109/ACCESS.2021.3091327

[30] Alharby M, van Moorsel A. BlockSim: An extensible simulation tool for blockchain systems. Frontiers in Blockchain. 2020;3(June):1–16. Available from: 10.3389/fbloc.2020.00028

[31] Jiang S, Li X, Wu J. Hierarchical edge-cloud computing for mobile blockchain mining game. Proceedings - International Conference on Distributed Computing Systems. 2019;2019-July(April):1327–1336. Available from: 10.1109/ICDCS.2019.00133

[32] Chen Z, Qi X, Du X, Zhang Z, Jin C. PEEP: A parallel execution engine for permissioned blockchain systems. Lecture Notes in Computer Science (including Subseries Lecture Notes Artificial Intelligence Lecture Notes Bioinformatics). 2021;12683 LNCS(April):341–357. Available from: 10.1007/978-3-030-73200-4_24

[33] Chen Z, Zhuo H, Xu Q, Qi X, Zhu C, Zhang Z, et al. Schain: A scalable consortium blockchain exploiting intra-and inter-block concurrency. Proc VLDB Endow. 2021;14(12):2799–2802. Available from: 10.14778/3476311.3476348.

[34] Tsoulias K, Palaiokrassas G, Fragkos G, Litke A, Varvarigou TA. A graph model based blockchain implementation for increasing performance and security in decentralized ledger systems. IEEE Access. 2020; 8:130952–130965. Available from: 10.1109/ACCESS.2020.3006383