UNIVERSIDAD TÉCNICA DE MACHALA

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

MAESTRÍA EN SOFTWARE

DESARROLLO DE UNA PLATAFORMA FINTECH UTILIZANDO TECNOLOGÍA DE REGISTRO DISTRIBUIDOS PARA EL ALMACENAMIENTO SEGURO DE TRANSACCIONES FINANCIERAS

ING. JIMMY FERNANDO CASTILLO CRESPÍN

TUTOR: ING. DIXYS HERNÁNDEZ, PHD

MACHALA

2022

UNIVERSIDAD TÉCNICA DE MACHALA

UNIDAD ACADÉMICA DE INGENIERÍA CIVIL

DESARROLLO DE UNA PLATAFORMA FINTECH UTILIZANDO TECNOLOGÍA DE REGISTRO DISTRIBUIDOS PARA EL ALMACENAMIENTO SEGURO DE TRANSACCIONES FINANCIERAS

ING. JIMMY FERNANDO CASTILLO CRESPÍN

PROYECTO TECNOLÓGICO AVANZADO

TUTOR: ING. DIXYS HERNÁNDEZ, PHD

COTUTOR: ING. FÉLIX FERNÁNDEZ, PHD.

MACHALA

2022

PENSAMIENTO

“No hay peor derrota que perder sabiendo que no te esforzaste lo suficiente.”

Ing. Jimmy Fernando Castillo Crespín

DEDICATORIA

Dedico este trabajo, primeramente, a Dios, por brindarme la salud y fuerza necesaria para lograr cumplir todas mis metas propuestas durante la duración del periodo de mi maestría en software.

A mis padres, aquellos que me dieron la vida y siempre están ahí cuando se los necesita, tanto en momentos malos como en los buenos, resaltando todo su apoyo, consejos y ánimos entregados hacia mí día tras día.

A mi hermano, porque al igual que mis padres, me entregó todo su apoyo, ánimos y comprensión, lo cual me motivaron mucho para el cumplimiento de mis objetivos.

Ing. Castillo Crespín Jimmy Fernando.

AGRADECIMIENTO

Agradezco, primeramente, ante todo a Dios, el cual durante todo el transcurso de mi vida me ha dado fuerza, salud y me ha guiado por el camino del bien tanto en las cosas que me he propuesto realizar y en las decisiones que se me han presentado en mi convivir diario.

Agradezco a mi familia, los cuales son los seres más importantes en mi vida, ellos supieron criarme con los mejores valores y me han brindado sus apoyos tantos emocionales como económicos.

A los docentes de la Maestría en Software, por compartir los conocimientos y experiencias profesionales que han aportado considerablemente en mi formación profesional y académica.

A mis compañeros de maestría, los cuales a través de sus experiencias compartidas a lo largo de la duración de la maestría eh aprendido de ellos.

A la Universidad Técnica de Machala por darme la oportunidad de cursar mi Maestría en Software en una buena institución educativa, con buen ambiente y docentes.

Mi especial agradecimiento a mi tutor Ing. Dixys Hernandez, PHD, por su dedicación, conocimientos y apoyo hacia mí durante sus tutorías.

Ing. Castillo Crespín Jimmy Fernando.

RESPONSABILIDAD DE AUTORIA

Yo, Jimmy Fernando Castillo Crespín con C.I 0706829116, declaro que el trabajo de “”, en opción al título de Magister en Software, es original y auténtico; cuyo contenido: conceptos, definiciones, datos empíricos, criterios, comentarios y resultados son de mi exclusiva responsabilidad.

_____

Ing. Jimmy Fernando Castillo Crespín
CI: 0706829116

Machala, 2021/10/09

REPORTE DE SIMILITUD TURNITIN

CERTIFICACION DEL TUTOR

Yo, Dixys Leonardo Hernández Rojas con CI: 0923026298 tutor del trabajo de "Desarrollo de una plataforma Fintech utilizando tecnología de registro distribuidos para el almacenamiento seguro de transacciones financieras", en opción al título de Magister en Software, ha sido revisado, enmarcado en los procedimientos científicos, técnicos, metodológicos y administrativos establecidos por el Centro de Posgrado de la Universidad Técnica de Machala (UTMACH), razón por la cual doy fe de los méritos suficientes para que sea presentado a evaluación.

_____

Dixys Leonardo Hernández Rojas
C.I: 0923026298

Machala, 2021/10/09

CESIÓN DE DERECHOS

Yo, Jimmy Fernando Castillo Crespín con C.I: 0706829116, autor del trabajo de titulación “Desarrollo de una plataforma Fintech utilizando tecnología de registro distribuidos para el almacenamiento seguro de transacciones financieras”, en opción al título de Magister en Software, declaro bajo juramento que:

- El trabajo aquí descrito es de mi autoría, que no ha sido presentado previamente para ningún grado o calificación profesional. En consecuencia, asumo la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.
- Cede a la Universidad Técnica de Machala de forma exclusiva con referencia a la obra en formato digital los derechos de:
    a) Incorporar la mencionada obra en el repositorio institucional para su demostración a nivel mundial, respetando lo establecido por la Licencia Creative Commons Atribution-NoCommercial – Compartir Igual 4.0 Internacional (CC BY NCSA 4.0); la Ley de Propiedad Intelectual del Estado Ecuatoriano y el Reglamento Institucional.
    b) Adecuarla a cualquier formato o tecnología de uso en INTERNET, así como correspondiéndome como autor la responsabilidad de velar por dichas adaptaciones con la finalidad de que no se desnaturalice el contenido o sentido de la misma.

_____

Ing. Jimmy Fernando Castillo Crespín

CI: 0706829116

Machala, 2021/10/09

RESUMEN

En el campo de las aplicaciones Fintech, han ocurrido problemas de estafas, fraudes y robo de información especialmente en los años 2020 - 2021 por la aparición del COVID-19 debido al crecimiento de pequeños empresarios que se volcaron a manejar sus negocios de manera online y a su vez, aumentando la demanda de los clientes e indirectamente de la ciberdelincuencia. El principal problema con muchas aplicaciones Fintech son las vulnerabilidades detectadas en los procesos de transporte y almacenamiento de información, dado a que almacenan la información en bases de datos centralizadas muchas de las veces sin encriptar que son más propensas al robo, fraude o manipulación y aunque se han propuesto distintos métodos de seguridad para mitigar estas vulnerabilidades, el problema sigue latente. En años recientes se ha promovido el uso de los DLT (tecnología de contabilidad distribuida) como una nueva forma de protección de datos dado a las ventajas que ofrece como almacenamiento distribuido, uso de métodos criptográficos que garantizan seguridad, inmutabilidad y encriptación de la información. Por tal motivo, el presente trabajo detalla la implementación de una plataforma tecnológica Fintech bajo una arquitectura on cloud utilizando DLT para la seguridad en el transporte y almacenamiento de transacciones financieras realizadas cotidianamente en la pasarela de pagos "Pagar es Fácil". Tomando en consideración los diferentes tipos de DLT existentes, se eligieron las plataformas de IOTA y Tatum como plataformas DLT por ser soluciones robustas, gratuitas y con gran potencial de escalabilidad; para el desarrollo de las aplicaciones web y móvil se siguió la metodología Agile Block Chain Dapp Engineering; se utilizó IONIC como framework para la aplicación móvil, Laravel como framework backend, VueJs como framework frontend, arquitectura de Google en servidores, firebase como base de datos y el framework expressJS para la programación de los endpoints de conexión entre las aplicaciones desarrolladas y la API de Iota y Tatum para el envío y almacenamiento de información. En la ejecución del prototipo, se tomaron en cuenta las transacciones realizadas por los usuarios de Pagar es Fácil desde la implementación de los DLT, también se aplicaron diferentes pruebas de seguridad en conjunto con la certificación PCI-DSS de nivel 3 para la evaluación de seguridad de la aplicación. Tras el análisis de los resultados, se concluye que el uso del DLT provee alta seguridad en el transporte y almacenamiento de transacciones financieras en aplicaciones Fintech.

Palabras claves: blockchain, fintech, DLT, IOTA, Tatum, tangle.

ABSTRACT

In the field of Fintech applications, there have been problems of scams, fraud and information theft especially in the years 2020 - 2021 due to the emergence of COVID-19 due to the growth of small entrepreneurs who turned to manage their businesses online and in turn, increasing the demand of customers and indirectly of cybercrime. The main problem with many Fintech applications are the vulnerabilities detected in the processes of transport and storage of information, since they store the information in centralized databases, often unencrypted, which are more prone to theft, fraud or manipulation, and although different security methods have been proposed to mitigate these vulnerabilities, the problem remains latent. In recent years, the use of DLT (distributed ledger technology) has been promoted as a new form of data protection due to the advantages it offers such as distributed storage, use of cryptographic methods that guarantee security, immutability and encryption of information. For this reason, this paper details the implementation of a Fintech technological platform under an on cloud architecture using DLT for the security in the transport and storage of financial transactions performed daily in the payment gateway "Pagar es Fácil". Taking into consideration the different types of existing DLT, the IOTA and Tatum platforms were chosen as DLT platforms because they are robust, free solutions with great scalability potential; the Agile Block Chain Dapp Engineering methodology was used for the development of the web and mobile applications; IONIC was used as framework for the mobile application, Laravel as backend framework, VueJs as frontend framework, Google architecture in servers, firebase as database and the expressJS framework for programming the connection endpoints between the developed applications and the Iota and Tatum API for sending and storing information. In the execution of the prototype, the transactions carried out by the users of Pagar es Fácil since the implementation of the DLTs were taken into account; different security tests were also applied in conjunction with the PCI-DSS level 3 certification for the security evaluation of the application. After analyzing the results, it is concluded that the use of DLT provides high security in the transport and storage of financial transactions in Fintech applications.

Keywords: blockchain, fintech, DLT, IOTA,Tatum, tangle.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Desde su creación hace más de 30 años, el internet ha revolucionado el mundo tal y como lo conocemos, actualmente es un fenómeno mundial que influye sobre casi todos los ámbitos de la sociedad, en especial en el campo del comercio electrónico o e-commerce donde se realizan transacciones financieras de manera online desde la comodidad del hogar. Cabe recalcar que los métodos de pagos online mayormente utilizados por las personas en la actualidad son: tarjeta de crédito o débito proporcionadas por los bancos, las pasarelas de pagos que nacieron como una forma de realizar pagos más seguros y rápidos siendo Paypal una de las más sobresalientes y utilizadas por la mayoría de los negocios e-commerce [1] al igual que las transferencias bancarias, pero la que está teniendo más auge actualmente son las billeteras virtuales de criptomonedas utilizados principalmente para el trading y compra/venta de activos digitales [2]. Existe una constante que no puede dejarse de lado en cualquiera de las formas de pagos online mencionadas anteriormente y es que se han detectado un aumento progresivo de fraudes, estafas y robo de información tanto personal como de las tarjetas [3], estos problemas ocasionarían que las personas dejen de confiar en realizar compras online afectando así a millones de aplicaciones Fintech. Por tal razón, la comunidad científica ofrece soluciones aplicada a la seguridad en las transacciones financieras online como encriptaciones avanzadas y aprobadas mundialmente como AES o RSA para la protección de la información desde el lado del cliente, base de datos criptográficas en la nube como IOTA stronghold utilizada para la protección de secretos digitales (tokens, passwords etc) [4] y el uso de los DLT (tecnología de contabilidad distribuida) como una nueva forma de protección de datos dado a las ventajas que ofrece como almacenamiento distribuido, uso de métodos criptográficos que garantizan seguridad, inmutabilidad y encriptación de la información [5]. Brindar seguridad en los pagos online es de especial importancia debido a que potenciaría el uso de aplicaciones Fintech para el crecimiento económico de pequeñas y medianas empresas.

La propuesta de esta investigación surge tras las alertas de robos, fraudes y estafas en transacciones financieras online ocurridas especialmente entre los años 2020-2021 debido a la aparición del COVID-19 [6], esta pandemia mundial ha sido positiva en cierta medida para la industria de pagos digitales, según cifras de Mastercad y Americas Market Intelligence [7], se duplicó el número de personas que se volcaron a las transacciones online pasando del 45% al 83%, la explicación para este comportamiento es sencillo, las

cuarentenas impuestas por los gobiernos mundiales obligaron a las personas a realizar pagos online, potenciando indirectamente el crecimiento exponencial de las aplicaciones Fintech [8]. El COVID-19 también afectó significativamente el mercado de las criptomonedas [9] detectándose un incremento de usuarios y de mercados Fintech que se volcaron al trading de estas [10] y a su vez el interés de los hackers por encontrar vulnerabilidades en estas [11].

Los datos generados por las aplicaciones Fintech durante las transacciones financieras son de alto valor y contienen información sensible en muchos aspectos y es de conocimiento público por noticias o artículos de los últimos años, los constantes robos de información, fraudes y estafas cometidas por estas aplicaciones que no implementan un sistema de seguridad robusto. Por tal motivo, acceder a estos datos tanto personales como financieras es un objetivo primordial para los hackers de todo el mundo. Estas vulnerabilidades se encuentran bien detalladas en el trabajo realizado por los autores Kaur, LashKari & Habibi [12], donde concluyeron que hasta en la actualidad aún siguen existiendo vulnerabilidades humanas, tecnológicas y de transacciones presentes en aplicaciones financieras. Los mismos autores Kaur, LashKari & Habibi [13] en otro de sus artículos dieron más ejemplos de amenazas cibernéticas y las motivaciones que impulsan estos incidentes, aplicaron varias metodologías de modelado de amenazas como STRIDE, TRIKE, VAST y PASTA para mitigar ataques en diferentes aplicaciones Fintech, sin embargo, esto no bastó para mitigar por completo todas las amenazas. Finalmente, el trabajo de los autores Huh, Cho & Kim [14] donde se implementó un sistema de encriptación de datos utilizando RSA para la protección de llaves privadas generados por Ethereum, una de las plataformas blockchain más populares actualmente, incluso en este trabajo no se han tomado en consideración otras medidas de seguridad presentes en los trabajos de Kaur, LashKari & Habibi. Quedó en claro en trabajos anteriores que existen muchas plataformas Fintech que no son óptimas para realizar transacciones financieras, inclusive cuando estas transaccionan con criptomonedas [15], surgiendo soluciones como los contratos inteligentes o smart contracts para la mitigación de fraudes y estafas financieras, siendo la red Ethereum la más utilizada para esta labor [16] [17]. Este asunto tan importante ha sido ignorado por la mayoría de empresas desarrolladoras de software por el afán de lanzar aplicaciones Fintech y ganar mercado en estos tiempos de pandemia [18].

En el trabajo realizado por Gatteschi [19] discute las ventajas y desventajas del blockchain y concluye que esta tecnología puede ser aplicada en cualquier sector, brindando grandes ventajas al sector Fintech [20]. Pero surgen varias limitantes sobre el uso de la tecnología blockchain demostradas por los autores Gatteschi [19] y Mesengiser & Miloslavskaya [21] que podrían ser un problema a futuro para las aplicaciones Fintech y son el rendimiento y sostenibilidad con el medio ambiente, con respecto al rendimiento, mientras más crece la red de blockchain, mayor será el tiempo de procesamiento de la transacción, Bitcoin, por ejemplo, tiene la capacidad de procesar transacciones por segundo muy bajas dependiendo del congestionamiento de la red [22] a comparación de las 65.000 transacciones por segundo reportas por la empresa Visa en este año [23], esto afectaría a las aplicaciones Fintech debido a que las mayorías de estas, son aplicaciones móviles y requieren que estas transacciones sean rápidas y sean reflejadas al usuario en el menor tiempo posibilidad sin afectar la usabilidad. Con respecto al daño ambiental, los autores Vries & Stoll [24] y Vries [25] analizaron los daños ambientales producidos por las criptomonedas mayormente desarrollados bajo la tecnología blockchain, siendo estos daños exponenciales para el medio ambiente, esta limitante ocasionaría un problema para muchas aplicaciones, incluidas las Fintech, dado a que a futuro muchas personas, empresas o instituciones gubernamentales como el gobierno de China por ejemplo [26], rechacen utilizar, apoyar o colaborar con aplicaciones desarrollados bajo la tecnología blockchain por el daño al medio ambiente que este ocasiona.

Es indiscutible que la utilización del blockchain proporciona una solución robusta, gratuita y segura pero esta tecnología por sí misma no es suficiente, debe ser combinada con otros sistemas de seguridad [27], esto se debe a las diferentes tecnologías existentes de las cuales están desarrolladas las diferentes aplicaciones que requieren protecciones tanto a nivel de servidores como de aplicación. A raíz de esto surgió IOTA como solución a los problemas de rendimiento y sostenibilidad presentes en blockchain pero esta tecnología igualmente presenta sus limitaciones ocasionadas por ser una tecnología relativamente nueva [28].

Como se detalló anteriormente, se debe tomar en cuenta las limitaciones de rentabilidad y sostenibilidad ofrecidas por la blockchain que afectaría negativamente a las aplicaciones Fintech en un futuro, la rentabilidad será menor a medida del crecimiento del blokchain dado a que genera un abismal consumo energético debido al tiempo que a estos le toman para resolver operaciones matemáticas complejas para concatenarse a la

red [29] y a su vez generan residuos electrónicos [30]. Estos problemas se estudiaron mejor en la investigación realizado por Vries & Stoll [24] donde cuantificaron que toda la red del bitcoin genera por año una cantidad de 30,7 kilotoneladas de residuos electrónicos, que, según estos mismos autores, esta cantidad es comparable con los desperdicios generados por equipos electrónicos pequeños del país de Holanda. Entre las soluciones propuestas se encuentran diseñar estrategias de sostenibilidad ambiental para el blockchain propuesta por Bai & Sarkis & Cordeiro [31], los mismo autores Vries & Stoll [24] dan una solución de sustituir el sistema de minera (el protocolo Proof-of-work) en su totalidad, dado a que según los estudios realizados por los autores Nair & Dorai [32] y Gemeliarana & Sari [33] donde evaluaron el rendimiento y la seguridad que proporcionaba este protocolo en la red blockchain, siendo estos muy seguros pero su rendimiento será bajo y su costo eléctrico será alto dependiendo del crecimiento de la red, surgiendo de aquí propuestas como proof-of-contribution que reduce el consumo eléctrico al recompensar la dificultad de cálculo de un rompecabezas criptográfico [34] o el proof-of-stake que elimina la necesidad de batallar por resolver cálculos matemáticos por parte de los participantes sino que estas se ven limitadas por la cantidad de criptomonedas que poseen los participantes en sus billeteras [35].

Basados en las afirmaciones anteriores, la presente investigación utilizará el DLT de IOTA como solución a las problemáticas expuestas por los autores [19], [21], [29], [30] y [24], siendo IOTA la primera criptomoneda que se creó fuera del sistema blockchain [36], en su lugar utiliza Tangle que a diferencia del blockchain, solamente necesita confirmar dos transacciones de diferentes participantes para poder concatenar su transacción dentro del nodo de Tangle [37], resultando ser rentable para ser utilizado en aplicaciones Fintech debido a la rapidez en la confirmación de las transacción. El Tangle de IOTA hace posible que no exista la necesidad de utilizar la minería como en blockchain, con esto no afectaría al medio ambiente, en lugar de esto utiliza los propios dispositivos clientes como verificadores de transacciones, siendo perfecto para ser utilizado en el internet de las cosas (IoT) [38], [39] y en transacciones financieras debido a que no existen comisiones (fee) [40] que se carguen a las transacciones realizadas por los clientes en aplicaciones Fintech por citar un ejemplo. Lastimosamente, los Smart contracts de IOTA actualmente se encuentra en fase alfa [41], haciendo imposible su uso inclusive para pruebas, por tal motivo se hará uso de los smart contracts proporcionado

por la plataforma blockchain de Tatum para la demostración de la solución a la mitigación de estafas en compras online realizadas en marketplace.

Por todo lo anteriormente redactado y con la intención de colaborar con el objetivo 3.7 propuesto en el plan nacional de desarrollo [42] que incentiva a la producción y consumo ambiental de manera responsable con el fin de incrementar la productividad de tecnologías y así combatir con la obsolescencia programada y a su vez otorgar un adecuado uso y protección de la información proporcionada por los usuarios así como lo estipula el artículo 66 numeral 19 de la Constitución de la República del Ecuador [43] y la Ley Orgánica de Protección de Datos Personales [44] se realizó la presente que tiene como objetivo el desarrollo de una plataforma Fintech mediante la implementación de tecnología de registros distribuidos (DLT) para el almacenamiento seguro de transacciones financieras, partiendo de la hipótesis de que el uso de los DLT incrementa la seguridad de los datos en transacciones financieras y mitiga los fraudes y estafas producidos en compras online con tarjetas de crédito/débito utilizando los smart contracts en comparación a otros métodos tradicionales de seguridad utilizados actualmente.

Para el cumplimiento del objetivo detallado anteriormente, se diseñó una aplicación web y móvil las cuales se encuentran funcionando en arquitecturas cloud bajo la plataforma de Google, son diferentes instancias las cuales proporcionan una arquitectura basado en eventos y microservicios, estos microservicios proporcionan las Apis necesarias para el procesamiento de datos a través del protocolo https y la interfaz de programación API-REST y a su vez estos se encargarán de realizar el almacenamiento de los datos en los DLT utilizando IOTA cuando se trate de transacciones financieras realizadas con tarjetas de crédito/débito y smart contracts proporcionado por Tatum cuando se trate de compras realizadas en el marketplace y trading de criptomonedas en la plataforma de Pagar es Fácil.

La investigación se realizó en un ambiente de producción, tomando como objeto de estudio todas las transacciones realizadas por los usuarios en la plataforma de Pagar es Fácil evaluando los medios de transporte, almacenamiento y seguridad de los datos. Tras la aplicación de las pruebas pertinentes realizadas al finalizar la implementación de la propuesta se concluye que el Tangle de la plataforma de IOTA y de igual forma el Blockchain proporcionado por la plataforma Tatum otorgan un alto nivel de seguridad tanto en el almacenamiento como en el transporte de la información realizada por los usuarios en las transacciones financieras. Sin embargo, también se debe tener a

consideración las altas vulnerabilidades que se encuentran presentes cuando se utilizan pasarelas de pagos desarrollados por terceros. Se recomienda que estos procesos de pagos no solamente dependan de las bondades ofrecidas por blockchain o Tangle sino que también estos pagos tengan certificación PCI DSS mínimo de nivel 3, encriptación de datos de extremo a extremo y una certificación de seguridad como es la ISO 21000:2013.

La investigación se desarrollará en un total de 4 capítulos. El primer capítulo trata sobre el marco teórico y tiene como objetivo elaborar los antecedentes históricos, conceptuales y contextuales utilizados para el desarrollo del trabajo de titulación. El segundo capítulo indica todos materiales, métodos y metodologías que se utilizaron para esta investigación. En el tercer capítulo se detalla los resultados obtenidos durante el proceso y finalmente en el cuarto capítulo se realiza la discusión de los resultados obtenidos haciendo énfasis en los hallazgos fundamentales, relación con otros trabajos, conclusiones y sugerencias para trabajos futuros.

Bibliografía

[1] V. Creuz, «División financiera del trabajo en sistemas de pagos en Argentina y Brasil,» *Revista Geográfica Venezolana,* vol. 60, nº 2, pp. 430-445, 2019.

[2] A. Cortez y A. Tulcanaza, «BITCOIN: SU INFLUENCIA EN EL MUNDO GLOBAL Y SU RELACIÓN CON EL MERCADO DE VALORES,» *Revista Chakiñan de Ciencias Sociales y Humanidades,* nº 5, pp. 54-72, 2018.

[3] A. Pawlicka, M. Choraś, M. Pawlicki y R. Kozik, «A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic,» *Business Horizons,* 2021.

[4] IOTA, «IOTA Stronghold,» 2021. [En línea]. Available: https://stronghold.docs.iota.org/docs/welcome. [Último acceso: 2021].

[5] A. Panwar y V. Bhatnagar, «Distributed Ledger Technology (DLT): The Beginning of a Technological Revolution for Blockchain,» *2nd International Conference on Data, Engineering and Applications (IDEA),* pp. 1-5, 2020.

[6] J. D. N. I. M. A. H. Y. B. d. l. Á. &. V. M. J. A. Tello Saldaña, «Impacto de los canales de comercialización online en tiempos del COVID-19,» *INNOVA Research Journal,* vol. 5, nº 3, pp. 15-39, 2020.

[7] A. M. Intelligence, «La aceleración de la inclusión financiera durante la pandemia de COVID-19. Oportunidades ocultas que salen a relucir,» 2020. [En línea]. Available: https://www.mastercard.com/news/media/qdxlk0nc/ami_201016_mastercard_financial_inclusion_during_covid_es_short_03-1.pdf. [Último acceso: 2021].

[8] M. T. Le, «Examining factors that boost intention and loyalty to use Fintech post-COVID-19 lockdown as a new normal behavior,» *Heliyon,* vol. 7, nº 8, 2021.

[9] S. Lahmiri y S. Bekiros, «The effect of COVID-19 on long memory in returns and volatility of cryptocurrency and stock markets,» *Chaos, Solitons & Fractals,* vol. 151, 2021,.

[10] L. Y. M. A. N. Lan-TN Le, «Did COVID-19 change spillover patterns between Fintech and other asset classes?,» *Research in International Business and Finance,* vol. 58, 2021.

[11] C. F. Security, «Cybercrime in a time of coronavirus,» *Computer Fraud & Security,* vol. 2020, nº 5, pp. 1-3, 2020.

[12] G. Kaur, Z. H. Lashkari y A. H. Lashkari, «Cybersecurity Vulnerabilities in FinTech,» *Understanding Cybersecurity Management in FinTech. Future of Business and Finance. Springer, Cham,* pp. 89-102, 2021.

[13] G. Kaur, Z. H. Lashkari y A. H. Lashkari, «Cybersecurity Threats in FinTech,» *Understanding Cybersecurity Management in FinTech. Future of Business and Finance. Springer, Cham,* pp. 65-87, 2021.

[14] S. Huh, S. Cho y S. Kim, «Managing IoT devices using blockchain platform,» *19th International Conference on Advanced Communication Technology (ICACT),* pp. 464-467, 2017.

[15] D. Luo, T. Mishra, L. Yarovaya y Z. Zhang, «Investing during a Fintech Revolution: Ambiguity and return risk in cryptocurrencies,» *Journal of International Financial Markets, Institutions and Money,* vol. 73, 2021.

[16] G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali y R. Hierons, «Smart contracts vulnerabilities: a call for blockchain software engineering?,» *International Workshop on Blockchain Oriented Software Engineering (IWBOSE),* pp. 19-25, 2018.

[17] L. Liu, W.-T. Tsai, M. Z. A. Bhuiyan, H. Peng y M. Liu, «Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum,,» *Future Generation Computer Systems,* 2021.

[18] P. K. Ozili, «Financial Inclusion and Fintech during COVID-19 Crisis: Policy Solutions,» *The Company Lawyer Journal,* vol. 8, pp. 1-9.

[19] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda y V. Santamaría, «To Blockchain or Not to Blockchain: That Is the Question,» *IT Professional,* vol. 20, nº 2, pp. 62-74, 2018.

[20] W. (. Du, S. L. Pan, D. E. Leidner y W. Ying, «Affordances, experimentation and actualization of FinTech: A blockchain implementation study,» *The Journal of Strategic Information Systems,* vol. 28, nº 1, pp. 50-65, 2019.

[21] Y. Mesengiser y N. Miloslavskaya, «Problems of Using Redactable Blockchain Technology,» *Procedia Computer Science,* vol. 190, pp. 582-589, 2021.

[22] K. P. Tsang y Z. Yang, «The market for bitcoin transactions,» *Journal of International Financial Markets, Institutions and Money,* vol. 71, 2021.

[23] Visa, «VisaNet: el poder de conectar al mundo,» 2021. [En línea]. Available: https://www.visa.com.ec/la-diferencia-visa/impacto-global/visanet-poder-conectar-mundo.html. [Último acceso: 06 10 2021].

[24] A. d. Vries y C. Stoll, «Bitcoin's growing e-waste problem,» *Resources, Conservation and Recycling,* vol. 175, 2021.

[25] A. d. Vries, «Renewable Energy Will Not Solve Bitcoin’s Sustainability Problem,» *Joule,,* vol. 3, nº 4, pp. 893-898, 2019.

[26] G. Cao y W. Xie, «The impact of the shutdown policy on the asymmetric interdependence structure and risk transmission of cryptocurrency and China’s financial market,» *The North American Journal of Economics and Finance,* vol. 58, 2021.

[27] S. Gomathi, M. Soni, G. Dhiman, R. Govindaraj y P. Kumar, «A survey on applications and security issues of blockchain technology in business sectors,» *Materials Today: Proceedings,* 2021.

[28] M. Bhandary, M. Parmar y D. Ambawade, «Securing Logs of a System - An IoTA Tangle Use Case,» *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC),* pp. 697-702, 2020.

[29] J. A. PADILLA SÁNCHEZ, «Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos,» *Revista de Derecho Privado,* nº 39, pp. 175-201, 2020.

[30] N. O. Nawari y Shriraam Ravindran, «Blockchain and the built environment: Potentials and limitations,» *Journal of Building Engineering,* vol. 25, 2019.

[31] C. A. Bai, J. Cordeiro y J. Sarkis, «Blockchain technology: Business, strategy, the environment and sustainability,» *Business Strategy and the Environment,* vol. 29, nº 1, pp. 321-322, 2019.

[32] P. R. Nair y D. R. Dorai, «Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain,» *Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV),* pp. 279-283, 2021.

[33] I. G. A. K. Gemeliarana y R. F. Sari, «Evaluation of Proof of Work (POW) Blockchains Security Network on Selfish Mining,» *International Seminar on Research of Information Technology and Intelligent Systems (ISRITI),* pp. 126-130, 2018.

[34] T. Xue, Y. Yuan, Z. Ahmed, K. Moniz, G. Cao y C. Wang, «Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency,» *IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC),* pp. 636-644, 2018.

[35] S. A. Y. Chicaiza, C. N. S. Chafla, L. F. E. Álvarez, P. F. I. Matute y R. D. Rodriguez, «Analysis of information security in the PoW (Proof of Work) and PoS (Proof of Stake)blockchain protocols as an alternative for handling confidential nformation in the public finance ecuadorian sector,» *16th Iberian Conference on Information Systems and Technologies (CISTI),* pp. 1-5, 2021.

[36] P. Perazzo, A. Arena y G. Dini, «An Analysis of Routing Attacks Against IOTA Cryptocurrency,» *IEEE International Conference on Blockchain (Blockchain),* pp. 517-524, 2020.

[37] M. Bhandary, M. Parmar y D. Ambawade, «A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle,» *5th International Conference on Communication and Electronics Systems (ICCES),* pp. 827-832, 2020.

[38] W. F. Silvano y R. Marcelino, «Iota Tangle: A cryptocurrency to communicate Internet-of-Things data,» *Future Generation Computer Systems,* vol. 112, pp. 307-319, 2020.

[39] F. Guo, X. Xiao, A. Hecker y S. Dustdar, «Characterizing IOTA Tangle with Empirical Data,» *IEEE Global Communications Conference,* pp. 1-6, 2020.

[40] B. M. Agostinho, M. M. Pereira, A. P. Back, A. S. R. Pinto y M. A. R. Dantas, «Iota vs. Ripple: A Comparison Inside An Economy of Things Architecture for Industry 4.0,» *IEEE 6th World Forum on Internet of Things (WF-IoT),* pp. 1-6, 2020.

[41] IOTA, «Blog IOta,» 2021. [En línea]. Available: https://blog.iota.org/iota-smart-contracts-protocol-alpha-release/. [Último acceso: 08 10 2021].

[42] D. Secretaría Nacional de Planificación y, «Plan Nacional de Desarrollo 2017-2021-Toda una Vida,» 2017. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/downloads/2017/10/PNBV-26-OCT-FINAL_0K.compressed1.pdf.

[43] E. Constitución de la República del, «Ministerio de Educación del Ecuador,» 2008. [En línea]. Available: https://educacion.gob.ec/wp-content/uploads/downloads/2012/08/Constitucion.pdf. [Último acceso: 05 10 2021].

[44] A. N. d. Ecuador, «Ley orgánica de datos personales,» 2021. [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf. [Último acceso: 30 09 2021].