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 "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, 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, 2021/11/04

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.

_____

Ing. Dixys Leonardo Hernández Rojas, PHD
C.I: 0923026298

Machala, 2021/11/04

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, 2021/11/04

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 los últimos años se ha impulsado el uso de los DLT (tecnología de contabilidad distribuida) como 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 y mitigación de estafas en 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, IoTex y Tatum como plataformas DLT por ser soluciones robustas, gratuitas y con gran potencial de escalabilidad; para la aplicación 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, IoTex y Tatum para el almacenamiento y seguridad 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. Luego de analizar los resultados, se concluye que el uso del DLT otorga una 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 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 and mitigation of fraud in financial transactions performed daily in the payment gateway "Pagar es Fácil". Taking into consideration the different types of existing DLT, the IOTA, IoTex and Tatum platforms were chosen as DLT platforms because they are robust, free solutions with great scalability potential; for the web and mobile application the Agile Block Chain Dapp Engineering methodology was followed; 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 the programming of the connection endpoints between the developed applications and the API of Iota, IoTex and Tatum for the storage and security of information. In the execution of the prototype, the transactions made by the users of Pagar es Fácil since the implementation of the DLTs were taken into account, also different security tests were 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 DLTs 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 y actualmente influye en muchos ámbitos sociales, 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 la confianza de los usuarios en el uso de aplicaciones Fintech.

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. Se evidencia que, en los trabajos anteriormente citados, muchas plataformas Fintech no cuentan con la seguridad suficiente 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 aplicar solamente blockchain no es suficiente, hay que implementarla en conjunto con otros métodos de seguridad [27], esta problemática surge por las variadas 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 blockchain 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 están 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 beta [41], haciendo posible su implementación en un ambiente de pruebas, pero imposible para producción, por tal motivo se hará uso de los smart contracts proporcionado por IoTex para la demostración

de la solución a la mitigación de fraudes y estafas en operaciones financieras realizadas con tarjetas de crédito o débito.

En base al trabajo de Taylor & otros [42] donde se realizó una revisión sistemática literaria de las ventajas de seguridad cibernética ofrecidas por la utilización del blockchain y en base al trabajo realizado por Ali & otros [43] donde muestran el estado actual de la utilización de la tecnología DLT en el sector financiero, se estableció el objetivo de esta investigación que busca la implementación de los DLT en aplicaciones Fintech para el almacenamiento seguro de las transacciones financieras, tomando en cuenta que la tecnología DLT estará presente en el futuro de la ciberseguridad financiera [44].

Por todo lo anteriormente redactado y con la intención de colaborar con el objetivo 3.7 propuesto en el plan nacional de desarrollo ecuatoriano [45] 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 una adecuada utilidad a la información confidencial de los usuarios así como lo estipula el art. 66, #19 de la Constitución del Ecuador [46] y la Ley de Protección de Datos (LOPD) [47] se realizó esta investigación que tiene como objetivo la implementación de tecnologías de registros distribuidos (DLT) para el almacenamiento seguro de las transacciones financieras realizadas en todas las funcionalidades proporcionadas por la plataforma Fintech Pagar es Fácil, partiendo de la hipótesis de que utilizar DLT otorgará ventajas como seguridad, inmutabilidad, integridad, no repudio, disponibilidad y confidencialidad de los datos generados en las transacciones financieras de la plataforma anteriormente mencionada, mitigando los fraudes y estafas producidos por usuarios al realizar operaciones financieras con tarjetas de crédito/débito utilizando el almacenamiento con coste cero de Tangle de IOTA y los smart contracts de la plataforma Tatum con blockchain.

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 que gracias a su coste cero en sus almacenamientos será utilizado cuando se trate de transacciones financieras generales, se programarán smart contracts utilizando IoTex cuando se trate de compras realizadas en el marketplace y trading de criptomonedas y finalmente se utilizará Tatum como plataforma blockchain para la transferencias internas y externas de criptomonedas.

La investigación se realizará en un ambiente de producción, tomando como caso práctico todas las transacciones realizadas por los usuarios en la plataforma de Pagar es Fácil evaluando aspectos como el transporte, almacenamiento y seguridad de la información confidencial de los usuarios. Luego de 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 IoTex y la plataforma Tatum mejoraron la seguridad y mitigaron fraudes y estafas realizadas por los usuarios en sus transacciones financieras dentro de la plataforma Fintech. 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 siguiente investigación está estructurada en cuatro capítulos partiendo de la introducción donde se le indica al lector de lo que se va a desarrollar en este trabajo. En el capítulo 1, trata sobre la elaboración del estado de arte la cual está conformada por los antecedentes históricos, conceptuales y contextuales, todos enfocados a los objetos de estudios que son las Fintech y los DLT. El segundo capítulo indica todos materiales, métodos y metodologías que se utilizaron en la investigación como es el tipo de estudio realizada, los enfoques, la población y la muestra, los métodos teóricos, empíricos, materiales y técnicas estadísticas utilizadas. En el próximo capítulo se muestran los resultados obtenidos, fundamentados en los aportes prácticos y teóricos obtenidos en el capítulo dos. En el cuarto capítulo se discute los resultados obtenidos haciendo énfasis en aspectos como los hallazgos obtenidos, su relación con otros trabajos, conclusiones y sugerencias para trabajos futuros. Finalmente, se elaboraron las conclusiones obtenidas de la investigación realizada y la bibliografía correspondiente.

CAPÍTULO I: ESTADO DE ARTE

1.1 Antecedentes históricos.

Las transacciones financieras online tuvieron su nacimiento en el año 1979 gracias al inventor Michael Aldrich pero su idea fue puesta en producción en el año 1984 cuando la señora Jane Snowball realizó una compra por VideoTex [48], uno de los primeros sistemas e-commerce que implementaron las ventas online [49] naciendo a partir de aquí el término Fintech 1.0 [50]. Por los años 90 con la aparición de las primeras aplicaciones Fintech como Paypal y otras plataformas como Ebay, Amazon o Alibaba Group Holding donde se implementaron pagos online se da paso a las Fintech 2.0 con el objetivo de proporcionar soluciones al sector financiero y a su vez dar un gran salto en la industria tecnológica [51]. Pero a su vez, el número de estafas, fraudes y robo de información incrementaron en diversas formas por parte de hackers que siguen aún presentes en tiempos actuales tal y como lo detallan los autores [52], [12] y [13].

Con respecto a las estafas o fraudes, debido a que estas nuevas formas de pago implementadas en su mayoría por sistemas e-commerce para aquella época, no eran tecnológicamente maduras [53], muchas de las veces se firmaban contratos entre las partes interesadas para asegurarse de que nadie cometa fraude. Cuando se menciona la palabra contrato, lo primero en que se piensa es en un papel escrito donde se establecen ciertas condiciones que, al ser leídas y aceptadas por las partes implicadas, los firmantes se comprometen a cumplir con dichas condiciones [54]. Actualmente, aunque este proceso sigue siendo utilizado en aspectos legales en todo el mundo, se ha dado un importante avance en cuanto a la automatización, seguridad y garantías con respecto a los contratos físicos tradicionales debido al surgimiento de los smart contracts o contratos inteligentes que se llevan desarrollando desde 1997 gracias al criptógrafo Nick Szabo quién acuñó el término smart contract por primera vez, pero debido a las limitaciones tecnológicas de la época no fue factible su idea de desarrollar un sistema de pagos que llevase el concepto de los contratos tradicionales a lo digital [55]. Pero esta situación se volvió viable en el año 2009 con la aparición del bitcoin por Satoshi Nakamoto [56] gracias a la implementación de las Tecnologías de Registros Distribuidos (DLT, por sus siglas en inglés).

Antes del nacimiento del bitcoin, en el año 2008 las Fintech dieron un salto tecnológico con su versión 3.0, naciendo de aquí el término startups, empresas emergentes cuya

característica principal es tener proyectos de rápido crecimiento y vertiginoso [57] entre ellos, proyectos de tipo Fintech que debido a la creciente popularidad del bitcoin, muchas de estas aplicaciones se enfocaron en el trading de criptomonedas y esto fue conocido como la blockchain 1.0 [58].

Como se mencionó anteriormente, la idea propuesta por Szabo de implementar contratos inteligentes para la mitigación de estafas y fraudes en su tiempo no era posible, pero gracias al surgimiento de la blockchain 2.0 en el año 2013 fue factible realizarlo. Esta nueva versión del blockchain permitió la aplicación de esta tecnología a nuevos campos de investigación con la inclusión de los smart contracts, microtransacciones, smart property, aplicaciones descentralizadas (Dapps), organización autónoma descentralizada (DAOs) y corporaciones autónomas descentralizadas (DACs) [58] [59], siendo todas estas nuevas funcionalidades muy prácticas para la solución de posibles vulnerabilidades en aplicaciones informáticas. No cabe duda que la funcionalidad con mayor interés en el campo de las Fintech son los smart contracts dado al impulso que tuvo en el año 2014 gracias a la creación de Ethereum (plataforma open-source mayormente utilizada para programar contratos inteligentes [60]). Los smart contracts funcionan en un sistema descentralizado que no puede ser manipulado por ninguna de las partes implicadas en el contrato ni por organismos externos. El contrato se cumple por condiciones programadas, firmadas por las partes implicadas y enviada a una cadena de bloques donde se asegura inmutabilidad e indelebilidad [61] siendo perfecta para ser utilizada en compras por internet de un marketplace (plataforma donde múltiples tiendas ofrecen sus productos o servicios) por citar un ejemplo práctico.

Debido a estos grandes avances del blockchain, fue a partir del año 2015 que muchas entidades financieras decidieron invertir en la infraestructura blockchain. Entre las entidades más destacadas se encuentran: J.P Morgan Chase que creó una división enfocada enteramente al blockchain [62] de las cuales se obtuvieron como resultado su propia blockchain privada denominada Quorum desarrollado bajo el código Ethereum [63] y en el año 2019 lanzaron su propia criptomoneda llamada JPMCoin [64]. Cabe recalcar que Quorum fue diseñado para satisfacer las necesidades de las instituciones financieras [65]. Otro caso significativo de implementación del blockchain en instituciones financieras se dio en el año 2016 por parte del Banco Santander de España, cuando inició sus pruebas en conjunto con la Empresa Ripple (creadora de la criptomoneda XRP [66]) para desarrollar servicios de pagos internacionales dando como

resultado su servicio Fintech denominado Santander One Pay FX [67]. También es importante resaltar a otros bancos como The Hong Kong and Shanghai Banking Corporation (HSBC) de Reino Unido con su red privada blockchain FX Everywhere lanzada en el 2018, el Wells Fargo (EEUU) con su sistema Wells Fargo Digital Cash basado en blockchain R3, BTG Pactual (Brasil) con su token ReitBZ y Mitsubishi UFJ Financial Group (Japón) con su red privada blockchain Global Open Network y su criptomoneda MUFG Coin [68].

Pero no todo lo proporcionado por la blockchain 2.0 son ventajas, en los últimos 5 años se han elaborado artículos donde se detallan ciertos inconvenientes que a futuro serían un problema para todas las aplicaciones que utilicen blockchain y una de ellas es la rentabilidad. Para que un nodo sea considerado como válido dentro de la red deberá ser aprobado por más del 50% de nodos en la red blockchain (one-cpu-one-vote) [69] lo que quiere decir que, mientras más crezca la red, mayor será el tiempo de procesar una transacción, siendo esto ya no tan rentable para aplicaciones desarrolladas por startups o microempresas. De igual forma sucede con las comisiones o fee que se cobran por cada transacción. Estas comisiones no están reguladas y varían dependiendo de varios factores como el congestionamiento de la red, el valor de la criptomoneda [70] agregando un costo adicional, muchas de las veces exageradamente alto, a las transacciones realizadas por los usuarios. Como último inconveniente está el alto consumo de energía, esto se evidencia en los artículos elaborados por los autores [12], [13], [24], [25] & [31] y aunque existen soluciones como el Proof-of-work o Proof-of-stake para disminuir el consumo eléctrico, el problema de la sostenibilidad ambiental sigue presente en la actualidad.

Debido a estos problemas de rentabilidad, sostenibilidad y escalabilidad documentados en los últimos años por la utilización de los DLT, en el año 2017 se dio paso a una próxima evolución del blockchain, conocido como la blockchain 3.0 que son redes creadas para soportar aplicaciones descentralizadas pero con la ventaja de tener mayor capacidad que las redes pioneras del blockchain (bitcoin y Ethereum) [71] siendo la red Cardano (criptomoneda ADA) una de las más sobresalientes de esta nueva tecnología [72]. Aunque estas nuevas redes solucionan gran parte de estos problemas, no lo solucionan del todo, naciendo de aquí DLT IOTA como solución a todos los problemas mencionados anteriormente y es por esto que IOTA no es considerada un blockchain sino un Tangle basado en tecnología DAG (gráficos acíclicos dirigidos) [73].

Gracias al protocolo de consenso de IOTA, llamado FPC (Fast Probabilistics Consensus) [74], no existe distinción entre mineros y usuarios (ambos se consideran como nodos), haciendo que todos los nodos de la red sean participantes en operaciones computacionales que no requieren de mucho consumo de energía como almacenamiento y validaciones de transacciones, solucionando de esta manera el problema de la sostenibilidad ambiental dado por la tecnología blockchain. Al no existir los mineros, ya no existe la necesidad de pagar por una comisión (fee) cada vez que se realiza una transacción. Cada transacción realizada con IOTA tiene un coste cero o también conocido como fee con valor cero [75], haciéndolo perfecto para ser utilizado en micropagos de IoT [76] o para aplicaciones Fintech. En cuestión de la rentabilidad, en IOTA no se requiere que al menos el 50% de nodos de la red apruebe la transacción para unirla a la red. Cada usuario de IOTA puede realizar una transacción, pero para unirla a la red deberá validar al menos dos transacciones que antecederán a su nodo y posteriormente otro nodo validará la transacción inicial [77]. La ventaja de esto es que incrementa mucho la rentabilidad en las transacciones realizadas en cualquier aplicación, siendo más veloces, seguras y altamente escalables. Un aspecto negativo con respecto a IOTA, se debe a la carencia de implementación de los smart contracts, según el reporte del mes de octubre del 2021 de IOTA [41], los smart contract se encuentra actualmente en fase beta para los desarrolladores. Por lo tanto, Ethereum sigue siendo líder actualmente en la construcción de smart contracts [78].

Debido al surgimiento del COVID-19, las aplicaciones Fintech tuvieron un crecimiento considerable durante los años 2020-2021 [10]. Se registraron incrementos en la cantidad de usuarios que se inclinaron por realizar compras online e invertir en la bolsa de valores de criptomonedas [79], pero a su vez se detectaron un incremento de la ciberdelincuencia en estas aplicaciones [80], [81], [82], [83] & [84]. La implementación de los DLT en el campo de las Fintech, con todas las virtudes descritas anteriormente en esta investigación, surge como una medida extra de seguridad para dichas aplicaciones y aunque estas no logren solucionar todas vulnerabilidades por completo, es un esfuerzo adicional que la comunidad científica ofrece como protección a posibles ataques informáticos relacionados a las aplicaciones Fintech, como se muestra en el trabajo realizado por Angelis y Ribeiro da Silva [85] & Mohanta y otros [86]. Actualmente se está trabajando en la blockchain 4.0 en conjunto con la industria 4.0, que a pesar de que en esta investigación no se utilizará esta tendencia, la característica de inclusión de la inteligencia

artificial al blockchain [87] sería un gran avance para la mitigación de fraudes y estafas en transacciones financieras online. La figura 1 presenta una síntesis de los antecedentes históricos elaborado para esta investigación.

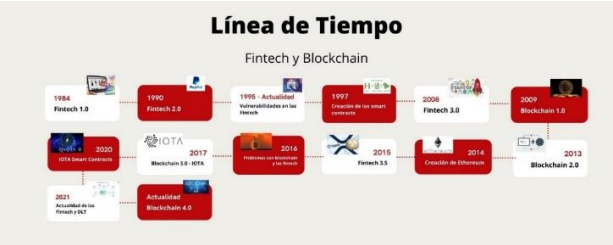

Figura 1: Organización cronológica de los antecedentes de las fintech y blockchain.

Fuente: Elaboración propia

1.2 Antecedentes conceptuales.

1.2.1 Hipótesis de la investigación.

Para esta investigación se elaboraron dos hipótesis, una de investigación (Hi) y otra nula (Ho) que serán analizadas durante el desarrollo de la investigación y su validez se mostrarán en el capítulo IV en la sección de discusión de resultados obtenidos.

Hi: La aplicación de tecnologías de registros distribuidos (DLT) incrementa la seguridad de los datos en el almacenamiento de las transacciones financieras en aplicaciones Fintech y así mitigar los casos de fraudes y estafas.

Ho: La aplicación de tecnologías de registros distribuidos (DLT) no incrementa la seguridad de los datos en el almacenamiento de las transacciones financieras en aplicaciones Fintech en la mitigación de casos de fraudes y estafas.

1.2.2 Red de categorías de las variables.

1.2.2.1 Variable independiente.

- Tecnologías de registros distribuidos (DLT).

1.2.2.2 Variable independiente.

- Seguridad de los datos en el almacenamiento de las transacciones financieras en aplicaciones Fintech.

En la figura 2 se muestran las variables de investigación seleccionadas para la presente investigación.

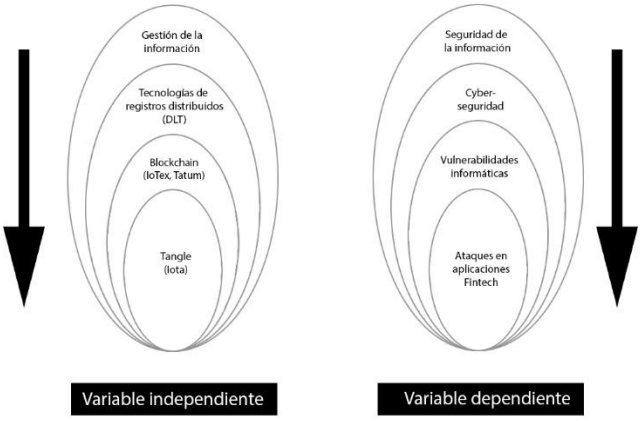

Figura 2: Variables dependientes e independientes seleccionadas

Fuente: Elaboración propia

1.2.3 Fundamentación teórica de la variable independiente.

Las maneras de almacenamiento fue la variable independiente seleccionada para esta investigación y como estas ayudarían a la seguridad de los datos personales y financieros en aplicaciones Fintech, partiendo desde lo más general como es la gestión de la información a lo más específico que son las tecnologías de registros distribuidos.

1.2.3.1 La gestión de la información.

También conocida como GI, se refiere a todos los procesos que intervienen en todo el ciclo de vida de los datos, partiendo desde su captura hasta su eliminación y durante ese proceso se incluyen tareas como extracción, combinación, depuración, almacenamiento y distribución de la información a todos los stakeholders [88]. El objetivo final de los GI es la garantización de la confidencialidad, disponibilidad e integridad de los datos [89], aspectos importantes a tener en cuenta en aplicaciones Fintech que se relacionan con la LOPD [47].

Para la gestión de la información se utiliza diferentes medios de almacenamiento como pueden ser base de datos no estructuradas, base de datos relacionales y no relacionales para salvaguardar la información pero actualmente se está optando por almacenarlo en la nube debido a su gran potencial de escalabilidad y seguridad para la información [90], naciendo los DLT como una nueva forma de almacenamiento para la gestión de la información, esta afirmación acerca del blockchain viene sustentada por los trabajos realizados por Yang [91] y Sheng [92].

1.2.3.1.1 Tecnologías de registros distribuidos (DLT).

Los DLT involucran varias tecnologías dando como resultado una base de datos que no es supervisada por ninguna entidad, es decir, es no centralizada, la ventaja de registrar cualquier tipo de información de manera descentralizada es el aumento de seguridad de los datos [93], ya que un hacker no podría acceder a esta información debido a que se encontraría distribuida en múltiples servidores. En la figura 3 se ilustra el funcionamiento de los DLT y se pondrá como contexto las aplicaciones Fintech en un ledger centralizado en comparación con un ledger descentralizado.

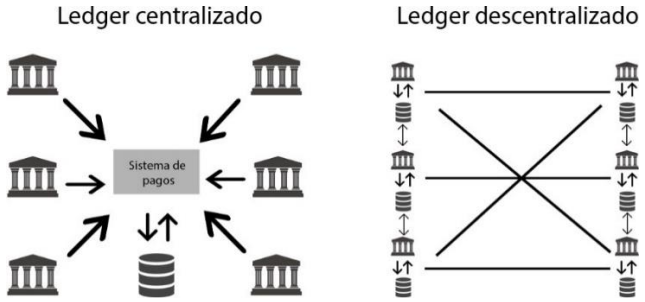

Figura 3: Ledger centralizado y descentralizado en un ambiente Fintech

Fuente: Elaboración propia

El autor Hashimy [94] detalla las ventajas más sobresalientes de los DLT de los cuales se encuentran que mejoran la eficiencia en la distribución de la información, también reduce los costos debido a que una institución ya no gastaría dinero en pagar servidores, sino que utilizaría el almacenamiento público de las redes de los DLT, al igual que la garantización de la inmutabilidad, trazabilidad, seguridad y transparencia de los datos almacenados.

En cuestión de su clasificación, el autor Zhuang [95] clasifica a los DLT en tres tipos, el blockchain, Tempo Ledger y DAG Ledger, en la figura 4 se muestra un organigrama elaborado por este mismo autor indicando los tipos de DLT y algunas tecnologías involucradas en ellas, es importante conocer esta clasificación debido a que en esta investigación se hará uso del blockchain y DAG como propuesta de solución y algo que llama la atención de la clasificación propuesta por Zhuang, es que coloca a IOTA como de tipo Tempo Ledger, esto entra a discusión con el autor Sadasiuvam [96] el cual indica que IOTA es un DAG al igual que HyperLedger Fabric que el autor Nawari [30] lo coloca de tipo blockchain y el autor Zhuang lo coloca de tipo DAG.

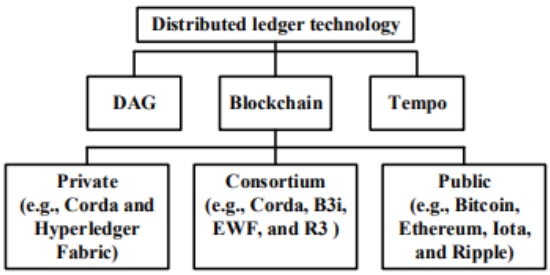

Figura 4: Clasificación de los DLT

Fuente: *[95]*

En la figura 5 elaborado por Bahar [97] proporciona más características de los DLT, una de ellas es su amplia aplicación en diferentes campos como puede ser en la medicina, Iot, finanzas, industrias y mucho más, demostrando la gran versatilidad de esta tecnología en ser aplicadas en muchos dispositivos tecnológicos (smart watch, celulares, laptos, routers etc). Actualmente existen dos estructuras en como la información en los DLT se distribuye dentro de la red, la primera es en forma de cadena de bloques como es el caso del blockchain y como DAG en el caso del Tangle [98] y cada una de ellas manejan sus propios protocolos de consenso entre las más destacadas se encuentran el proof-of-work, proof-of-stake, proof-of-contribution, FPC (IOTA) [99] y también ventajas únicas como la implementación de smart contracts muy baratas con IoTex blockchain [100] o un almacenamiento con coste cero con IOTA [38].

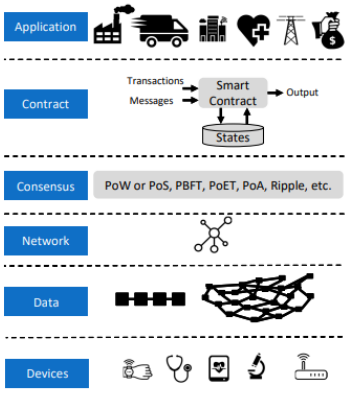

Fig. 2: DLT Stack.

Figura 5: Características de los DLT

Fuente: *[97]*

1.2.3.1.2 Blockchain.

El blockchain es considerado un libro de cuentas, donde cada registro es único, consensuado, distribuido y cifrado entre múltiples bloques que forman parte de la red

[101]. El autor Feng [102] la define como una base de datos distribuida que utiliza el P2P ofreciendo seguridad y privacidad en las transacciones que se registran, estas transacciones no solamente pueden ser económicas sino puede ser cualquier tipo de información proveniente de cualquier aplicación.

Para que el blockchain pueda funcionar requiere tener varios nodos que son considerados como mineros que se encargan de verificar estas transacciones utilizando diferentes protocolos de consenso para posteriormente validarlas y concatenarlas a la cadena de bloques [103].

1.2.3.1.2.1 Tipos de Blockchain.

La blockchain se encuentra clasificada en dos ámbitos, como son los permisos de acceso y la privacidad en los usuarios para verificar transacciones dentro de la red, esta clasificación se encuentra detallada a fondo en los trabajos realizados por [104] y [105] clasificándolos de la siguiente manera:

Permisos de acceso:

- Con permisos: Requiere autenticación para ingresar e interactuar con la red.
- Sin permisos: No requiere autenticación para ingresar e interactuar con la red.

Privacidad en transacciones:

- Transacciones públicas: cualquier persona puede ver las transacciones.
- Transacciones privadas: solo los usuarios pertenecientes a la red pueden ver las transacciones.

1.2.3.1.2.2 Ventajas del blockchain.

El autor Abdi & otros [106] detallaron en su trabajo muchas ventajas de la utilización de esta tecnología, convirtiéndola en primera opción para ser utilizada en muchos proyectos de diferentes áreas, entre las ventajas principales se destacan:

- Descentralización: las transacciones son procesados por múltiples servidores.
- Trazabilidad: los usuarios pueden estar pendientes del estado de sus transacciones.
- Transparencia: los datos no pueden ser alterados.
- Autonomía: los datos no son regulados por ninguna entidad.

1.2.3.1.2.3 Plataformas blockchain

Yang [105] y Nguyen [107] mencionan varias plataformas blockchain como:

- Bitcoin
- Ethereum
- Hyperledger Fabric
- Tatum
- IBM Blockchain
- Multichain
- Hydrachain
- Ripple
- R3 Corda
- Openchain

1.2.3.1.2.4 IoTex.

IoTex es una infraestructura de blockchain cuya principal característica es su protocolo de consenso en tiempo real llamado Roll-DPoS [108] la cual le permite una comunicación rápida y eficaz entre la blockchain y los millones de dispositivos conectados debido a que este protocolo utiliza un sistema de votación de minería de entre 21 a 50 delegados dentro de la blockchain y a su vez cada blockchain interactúa con diferentes dispositivos [109]. Gracias a este protocolo se obtiene una red con un rendimiento significativamente más alta y el costo por cada transacción es mucho menor en comparación a otras blockchain [100], haciéndola perfecta para ser utilizado para smart contracts por su rapidez y bajo costo en comisiones. En la figura 6 se muestra un ejemplo de smart contract con IoText.

```
import solc from "solc";

const solidityFileString = `
pragma solidity ^0.4.16;

contract SimpleStorage {
   uint storedData;

   function set(uint x) public {
       storedData = x;
   }

   function get() public view returns (uint) {
       return storedData;
   }
}
`;
const contractName = ":SimpleStorage";
const output = solc.compile(solidityFileString, 1);
const abi = JSON.parse(output.contracts[contractName].interface);
const bytecode = output.contracts[contractName].bytecode;
```

Figura 6: Ejemplo de un smart contract con iotex

Fuente: *Elaboración propia.*

1.2.3.1.2.5 Smart contracts.

Los contratos inteligentes o smart contracts son programas especiales que ejecutan instrucciones en redes distribuidas para almacenarlos en la blockchain y así asegurar que dicha información sea inmutable, transparente y seguras [110].

1.2.3.1.2.6 Solidity.

Solidity es un lenguaje de programación considerada de alto nivel que hizo posible la creación de las Dapps debido a que con este lenguaje hizo posible la programación de los smart contracts que generalmente se las utiliza con el EVM de Ethereum [111].

1.2.3.1.2.7 Tatum.

Según la definición de su web oficial, Tatum "es una plataforma opensource para simplificar el desarrollo de aplicaciones DLT soportando más de 40 protocolos de blockchain y activos digitales en una misma API" [112]. Tatum admite las siguientes redes de blockchain para su desarrollo e implementación [113]:

- Mainnet. - red principal del blockchain.
- Testnet. - red de pruebas del blockchain.
- Virtual accounts. - cuentas virtuales pertenecientes a la red privada de Tatum.
- Base chain. – otras cadenas de blockchain pertenecientes a otras billeteras.

En la figura 7 se contempla la infraestructura de Tatum, la cual está compuesta por tres principales partes, la infraestructura blockchain, la plataforma cloud de Tatum y librerías de desarrollo [114], brinda beneficios como facilidad de utilizar sus apis, prueba del futuro y escalabilidad en el desarrollo de aplicaciones.

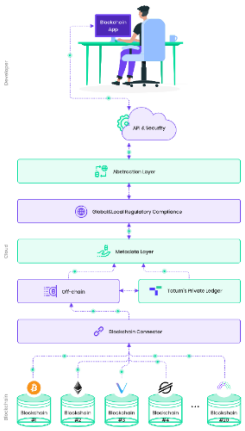

Figura 7: Arquitectura de Tatum

Fuente: [114]

1.2.3.1.3 Tangle DAG.

Tangle es el núcleo de la tecnología IOTA así como el blockchain lo es para el bitcoin o Ethereum y a diferencia del blockchain que utiliza una cadena de bloques, Tangle utiliza los DAG (gráficos acíclicos dirigidos) (ver figura 8) [115] el cual brinda mayores ventajas en los DLT como eliminar la necesidad de utilizar mineros debido a que utiliza los propios dispositivos clientes como nodos [116], su funcionamiento le permite hacer transacciones offline y posteriormente concatenarse a la red, es decir, cuando una transacción es enviada a la red de Tangle, debe aprobar dos transacciones y esperar a que otra transacción la apruebe y así formará parte de la red pero hasta eso los clientes pueden seguir enviando transacciones [117].

Entre las ventajas que ofrece Tangle, los autores [115], [116] & [117] concuerdan con la siguientes:

- Registra información de manera segura, transparente, inmutable.
- No cobra comisiones ya que no existe los mineros.
- Alta escalabilidad.
- Mejor rendimiento por la ejecución de transacciones en paralelo.
- Su arquitectura es más ligera que el del blockchain.
- Mientras más crezca el Tangle, más rápida será los procesos de verificación de transacciones.
- Descentralización y modular.

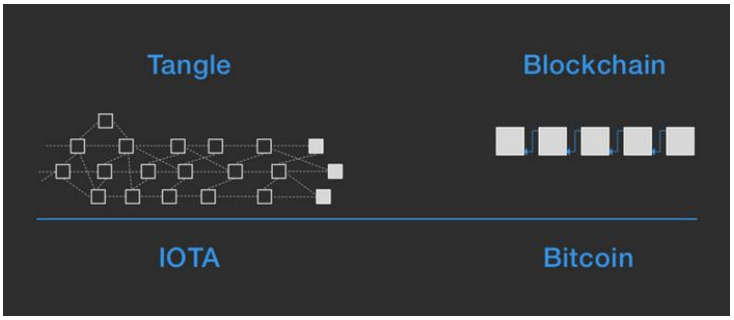

Figura 8: Arquitectura Blockchain vs Tangle

Fuente: *Elaboración propia.*

1.2.3.1.3.1 IOTA

Gracias al Tangle fue posible la creación de IOTA y goza de todas las características previamente argumentadas en esta investigación como la no dependencia de mineros, alta escalabilidad, cero costos en comisiones, descentralización. Iota es un DLT de código

abierto que nació para solucionar los múltiples inconvenientes del blockchain como son problemas de rendimiento, medio ambiente y alto costos en comisiones [118]. Su principal objetivo es la seguridad durante el flujo de la información en especial para el ambiente Iot [119].

Uno de los incovenientes con Iota es que no es totalmente descentralizada, cuenta con un nodo origen llamado coordinador que se encarga principalmente de evitar ataques de red [120] [121] pero esto se quiere solucionar con el nuevo protocolo conocido como chrysalis con la salida de IOTA 2.0 nectar reléase [122]. La ejecución de los Smart contracts es también otro punto negativo por el momento en IOTA, pero en octubre del 2021, IOTA Foundation dió la noticia de que los Smart contract se encuentran en su fase beta [41] dando un gran paso sobre esta arquitectura. Pero lo que hace posible todas estas ventajas en IOTA es gracias al protocolo de conseso utilizado en el Tangle llamado Fast Probabilistic Consensus (FPC), el cual según los creadores de este protocolo Serguei Popov y Bill Buchanan lo definen como un "protocolo de consenso binario probabilísticos el cual no posee líder, de baja complejidad comunicacional, convirtiéndolo en una tecnología robusta" [123].

1.2.4 Fundamentación teórica de la variable dependiente.

1.2.4.1 La seguridad de la información.

También conocida como S.I, nace para resguardar y proteger la información, donde se contempla un cúmulo de políticas de uso tanto preventivas como reactivas para el tratamiento de la información que se utilice dentro de alguna empresa y así evitar el acceso, utilización, divulgación o destrucción no autorizada de datos privados [124].

El objetivo principal de los S.I, según los autores Kirillova & otros [125] es garantizar de manera eficaz la protección de la información proveniente de los servicios, actividades, sistemas informáticos y comunicaciones dentro de una institución, protegiéndola contra violaciones que tengan que ver con la disponibilidad, integridad y confidencialidad de la información. Estos tres pilares se encuentran contemplados en la ISO/IEC 27001:2013 y para ponerlo en práctica las empresas identifican áreas con posibles vulnerabilidades de filtración de información, posteriormente evalúan los riesgos y finalmente otorgan los pasos necesarios para la reducción de los riesgos [126].

La detección de riesgos por lo general se los realiza en un ambiente de pruebas, el autor Wang [127] elaboró un marco tecnológico sobre la seguridad de la información realizados

en un ambiente de pruebas, donde se contempla aspectos relevantes que pueden ser de utilidad en la seguridad de aplicaciones Fintech como es el no repudio, integridad, seguridad de los datos, confidencialidad, seguridad de la red y estructural, en la figura 9 se muestran más aspectos del mismo.

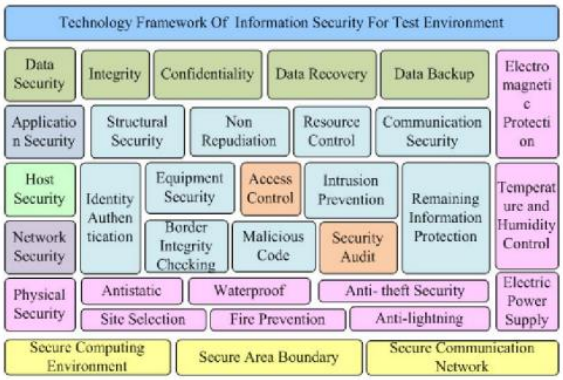

Figura 9: Framework de seguridad de la información para ambientes de pruebas

Fuente: *[127]*

1.2.4.2 Cyber seguridad.

La seguridad informática, según la Asociación de Auditoría y Control de Sistemas de Información (ISACA), es un nivel adicional de protección para la información, con este nivel se trabaja para mitigar cualquier amenaza ya sea interna o externa durante las fases de procesamiento, transportación y almacenamiento de la información desde cualquier dispositivo [128]. En cambio, el autor Tirumala [129] indica que la ciberseguridad consiste en proteger sistemas donde se gestiona información privada y sensible provenientes de diferentes medios como puede ser computadoras personales, servidores, redes informáticas, dispositivos móviles entre otros, de ataques digitales por parte de hackers, que, por lo general, logran acceder a puntos que no poseen la protección suficiente para modificar, eliminar o acceder a información personal para posteriormente extorsionar a los usuarios. Aunque a lo largo del tiempo se han implementado medidas de seguridad dentro de estos sistemas, los ataques informáticos siguen ocurriendo debido al aumento de las personas en utilizar dispositivos conectados a internet [130] y a la creatividad de los atacantes en utilizar la ingeniería social para penetrar sistemas [131].

1.2.4.3 Vulnerabilidades informáticas.

Las vulnerabilidades informáticas son todas aquellas que se originan cuando se produce un fallo o debilidad debido a una mala integración del software o hardware o simplemente

limitaciones presentadas por la tecnología por la cual fue desarrollado el software [132]. Estas vulnerabilidades son explotadas por hackers en lo que se conoce como ataques informáticos, accediendo sin autorización a diferentes sistemas informáticos mencionados anteriormente por el autor Tirumala, los atacantes una vez dentro del sistema, pueden comprometer los pilares de la seguridad de la información contemplados en la ISO/IEC 27001:2013.

Según Tundis [133], las vulnerabilidades informáticas pueden ser de tipo teórica y real, la real es conocida como los exploits, son fallos que se encuentran en muchas aplicaciones y sistemas operativos que son solucionados en próximas versiones.

Con la llegada de la cloud computing, muchas aplicaciones, especialmente del ámbito web, migraron a estas arquitecturas, apareciendo nuevas vulnerabilidades de las cuales el autor Kumar [134] elaboró un organigrama jerárquico (ver figura 10) detallando aspectos a tener en cuenta sobre la seguridad en la cloud computing, como los requerimientos, amenazas, vulnerabilidades y contra medidas que se deben considerar al utilizar esta arquitectura.

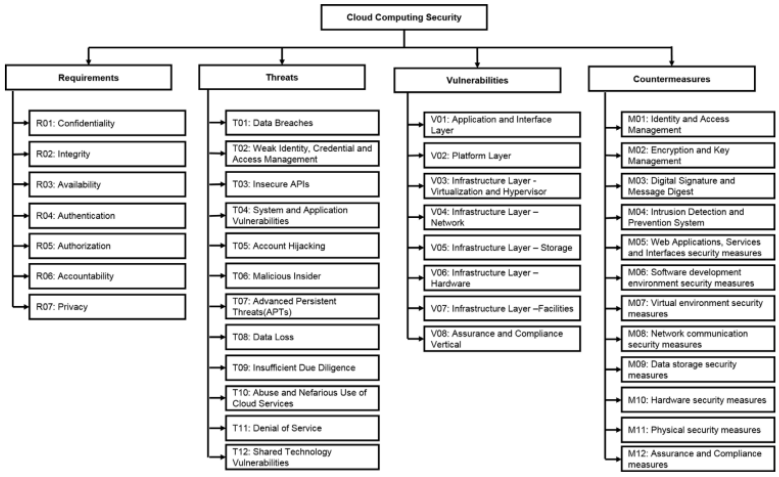

Figura 10: Seguridad en la cloud computing

Fuente: *[134]*

1.2.4.4 Ataques y vulnerabilidades en aplicaciones Fintech.

A lo largo de los años, han existido muchos ataques y amenazas informáticas pero debido a que en esta investigación se centrará en las aplicaciones Fintech, se ha recapitulado aquellas vulnerabilidades que ponen en los pilares de la información dentro de estas aplicaciones.

1.2.4.4.1 Falta de cifrado de datos.

Las aplicaciones Fintech gestionan información tanto personal como financiera de los usuarios, por tal motivo, se recomienda que toda información sensible viaje a través de la red, de manera cifrada utilizando algún algoritmo de cifrado ya sea simétrico o asimétrico como puede ser el AES, RSA o un híbrido, desde las aplicaciones cliente hasta los servidores y en el caso de que los servidores estén en la cloud, el autor Yang [135] recomienda aplicar algoritmos de cifrado como el KP-ABE o el CP-ABE dentro del cloud storage. Aunque no existe un algoritmo de cifrado mejor o peor que otro, la selección de este algoritmo dependerá del contexto de la aplicación, por lo tanto, para la aplicación Fintech de "Pagar es Fácil" se ha optado por la utilización del algoritmo asimétrico RSA dado a su ventaja de utilizar una llave pública para el cifrado de datos desde las aplicaciones clientes y aunque un hacker realice un ataque de hombre de en medio (man-in-the-middle) jamás podrá desencriptar la información ya que para esto necesitaría la llave privada que se encuentra solamente en los servidores [136], en la figura 11 se observa de manera gráfica el funcionamiento del algoritmo RSA. Esta característica del RSA lo hace perfecta para ser utilizada en aplicaciones móviles y Pagar es Fácil cuenta con una, debido a que si un atacante realiza una ingeniería inversa a la app móvil solamente obtendría la llave pública y no haría nada con ese dato, caso contrario pasaría si se usase un algoritmo simétrico AES que utiliza la misma llave para cifrar y descifrar los datos [137], si un hacker la obtiene podría fácilmente desencriptar toda la información que fluya entre las aplicaciones clientes.

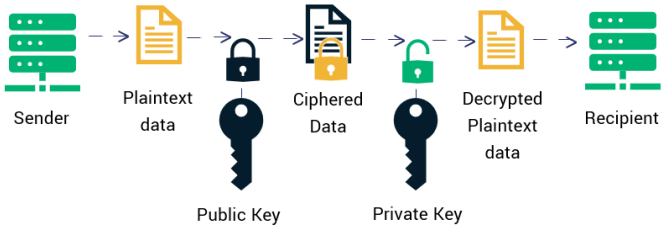

Figura 11: Algoritmo RSA

Fuente: Elaboración propia

1.2.4.4.2 Falta de doble factor de autenticación.

La doble autenticación es una medida de seguridad extra implementado actualmente por muchas aplicaciones, debido a que aparte de solicitar las credenciales de email/usuario y password se requerirá de un código obtenido por aplicaciones de tercero o servicios de mensajería como SMS o email [138].

La carencia de un doble factor de autenticación en una aplicación Fintech es claramente una vulnerabilidad alta, por eso se recomienda implementarlo ya sea registrando un código PIN o solicitarlo por la aplicación de Google Authenticator [139].

1.2.4.4.3 Ingeniería social.

La ingeniería social está presente en cualquier aplicación, en especial donde se maneja comunidades de usuarios y flujo de dinero, los atacantes utilizan una serie de técnicas como el phishing para engañar a los usuarios, por lo general envían links donde se encuentran formularios solicitándole sus datos confidenciales o inyectándole malware e infectar sus dispositivos [140] y así robar información como claves, cuentas de usuarios, datos de tarjetas de crédito entre otros.

1.2.4.4.4 Repudio de información.

El no repudio de la información es uno de los principios de la seguridad informática y consiste en garantizar al receptor que el mensaje es enviado por el emisor original y no otra persona [141], este aspecto es importante en las aplicaciones Fintech, ya que tener la capacidad de demostrar que los usuarios realmente realizaron las transacciones financieras es vital para evitar fraudes o estafas.

1.2.4.4.5 Carencia de seguridad en interfaces de programas de aplicación (API)

Actualmente, la mayoría de aplicaciones se construye bajo la arquitectura de microservicios, siendo la seguridad en las API un aspecto primordial en dichas arquitecturas pata proteger la confidencialidad de los datos que fluyen a través de estas API. Una API expuesta sin las seguridades suficientes son una de las principales causas de la filtración de datos confidenciales [142].

Entre las maneras propuestas para mitigar las vulnerabilidades en las API están las siguientes [143]:

- Encriptar el tráfico de red utilizando SSL-TLS- HTTPS.
- Que la API cuenta con un sistema de autenticación y autorización con token.
- Limitar el tráfico de llamadas con un API Gateway.
- Utilizar inteligencia artificial para detectar anomalías en el uso de las API.

1.2.4.4.6 Fraudes al utilizar tarjetas de créditos.

Esta vulnerabilidad va de la mano con el no repudio de la información, si la aplicación Fintech no cuenta con mecanismos para demostrar el no repudio de los usuarios al momento de utilizar sus tarjetas, claramente existirán los fraudes afectando económicamente a la empresa desarrolladora de la aplicación. En el ambiente web, existen tres tipos de fraudes con tarjetas que se deben tener a consideración [144]:

- Fraude en primera persona: se comete cuando la persona dueña de la tarjeta realiza un pago online pero luego se dirige al banco y miente diciendo que él no realizó dicho pago.
- Fraude en segunda persona: se comete cuando un amigo o alguien cercano al dueño de la tarjeta realiza un pago online sin el consentimiento del dueño.
- Fraude en tercera persona: se comete cuando el dueño de la tarjeta desconoce por completo quien fue la persona que realizo un pago online, en este caso el dueño de la tarjeta es claramente una víctima de la ciberdelincuencia.

1.2.4.4.7 Estafas al vender o comprar productos online.

Muchas grandes empresas como Alibaba, Facebook, Instagram, Amazon han optado por la utilización de los marketplaces, lugar donde muchas tiendas ofertan sus productos y debido a la razón de que cualquier persona puede crearse una tienda virtual dentro de estas plataformas, el alto índice de estafas en compras y ventas han aumentado debido a que no existe un ente regulador que compruebe que estas tiendas son reales y que los productos que se ofertan sean verídicas, esta información ha sido comprobada en varios artículos elaborados entre los años 2020-2021 citados en la sección de antecedentes históricos de esta investigación. Una propuesta de mitigación a esta problemática a sido la implementación de los smart contracts durante el proceso de compra.

1.2.4.4.8 Protección de seguridad del servidor web insuficiente.

Los autores Saraswat & Tripathi [145] comparten algunos beneficios por la utilización de servicios Paas o Iass en plataformas en la nube como Google, Microsoft Azure, IBM entre otros y entre estas ventajas se encuentran la seguridad ofrecida para las aplicaciones web, APIs y base de datos, quitando así un poco de peso a los desarrolladores en ya no preocuparse tanto por la seguridad de los servidores, cuestión que no sucedería si se optara por la utilización de servidores propios.

1.2.4.4.9 Incumplimiento del estándar PCI DSS.

El estándar PSI-DSS provee las mejores prácticas de seguridad y deben poseerla toda empresa que almacena, procesa o transmite información de datos de los dueños de las principales tarjetas de crédito en el mercado [146], un incumplimiento de este estándar ocasionaría pérdidas millonarias en las cuentas bancarias de los usuarios.

1.3 Antecedentes contextuales.

1.3.1 Delimitación del contexto de investigación.

La siguiente investigación se lo hará en un ambiente de producción, tomando como caso práctico todas las transacciones realizadas por los usuarios en las diferentes funcionalidades ofrecidas por la plataforma Fintech "Pagar es Fácil", que según su web oficial lo definen como un "eje de negocios digitales, enfocado principalmente a pequeños y medianos empresarios donde podrán comprar/vender productos o servicios, transaccionar con tarjetas de créditos y criptomonedas, poseer su propia billetera virtual, pagar servicios básicos entre otras funcionalidades" [147]. Su misión está enfocada en facilitar aspectos de negocios de los usuarios a través de procesos digitales de manera simple, rápida y segura. Su visión se centra en convertirse en el eje de negocios digitales más grande de América Latina [148], para esto, Pagar es Fácil requiere de la implementación de los DLT en todos sus procesos financieros para incrementar la seguridad de los datos transaccionales y a su vez mitigar los problemas de fraudes/estafas detectadas en las funcionalidades de los marketplace y en la utilización de tarjetas de crédito dentro de la plataforma por parte de los usuarios. Mientras más va creciendo la plataforma, más seguridad se debe implementar tanto en el transporte como en el almacenamiento de los datos que son puntos potenciales de ataques para hackers.

Actualmente, Pagar es Fácil cuenta con un aproximado de 125.00 usuarios (Ver figura 12) de los cuales se analizarán las transacciones realizadas en las siguientes funcionalidades detalladas en la Tabla 1 en conjunto con su propuesta de solución.

Figura 12: Cantidad de usuarios en Pagar es Fácil

Fuente: Datos estadísticos obtenidos de la plataforma.

1.3.2 Propuesta de solución.

Desde su creación hasta la actualidad, se han detectado vulnerabilidades en las aplicaciones Fintech, especialmente entre los años 2020-2021 por la presencia del COVID-19 y aunque la comunidad científica ha realizado investigaciones para aumentar la seguridad en estas aplicaciones, aún siguen existiendo estas vulnerabilidades.

La presente investigación pretende solucionar los problemas de estafas y fraudes en aplicaciones Fintech tomando como caso práctico la plataforma Pagar es Fácil, por tal motivo, 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.

La propuesta de solución consta de tres puntos:

- Utilizar IOTA que gracias a su coste cero en sus almacenamientos será utilizado en transacciones financieras generales, como pueden ser la utilización de tarjetas de créditos o movimientos del saldo de billetera dentro de la plataforma, se guardará en IOTA información como ubicación, ip, dirección, últimas conexiones entre otras informaciones de los usuarios para posteriormente ser utilizado como soporte para defenderse ante un posible reclamo de fraude por parte de las

entidades bancarias, en la figura 13 se detalla una primera versión de la arquitectura a utilizarse.

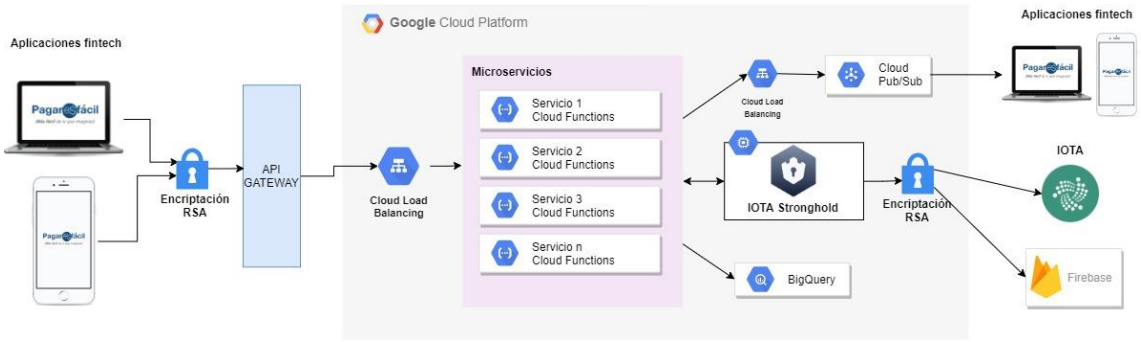

Figura 13: Arquitectura en transacciones financieras con IOTA

Fuente: Elaboración propia

- Se utilizará Tatum como plataforma blockchain para las transferencias internas y externas de criptomonedas y de igual forma se hará uso de IOTA para almacenar las transacciones realizadas y sea un soporte inmutable de los tradings realizados, en la figura 14 se detalla una primera versión de la arquitectura a utilizarse.

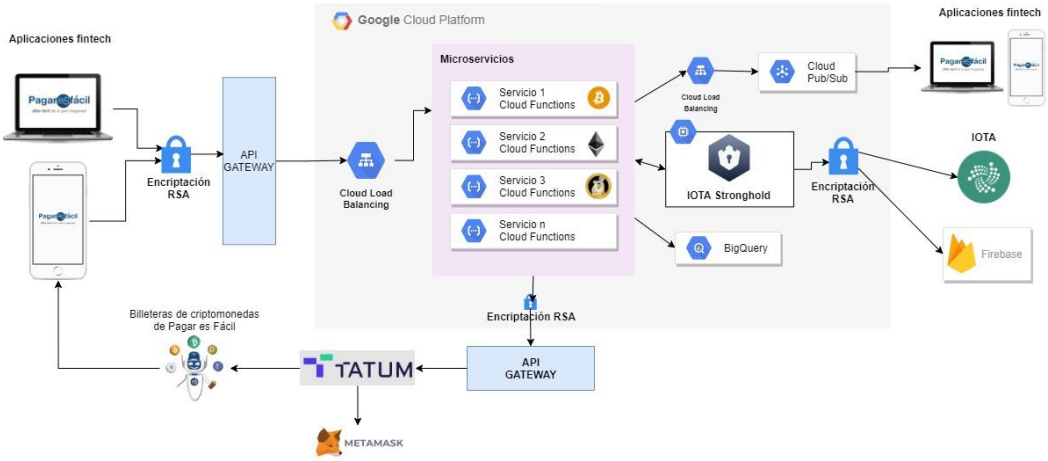

Figura 14: Arquitectura para transferencias internas y externas de criptomonedas

Fuente: Elaboración propia

- Finalmente, se programarán smart contracts para mitigar problemas de estafas utilizando IoTex blockchain cuando se trate de compras y ventas realizadas en el marketplace de productos/servicios y en el marketplace de criptomonedas donde se realizarán tradings y para eso también se hará uso de la plataforma Tatum. Las transacciones financieras resultantes serán almacenadas en IOTA, en la figura 15 se detalla una primera versión de la arquitectura a utilizarse.

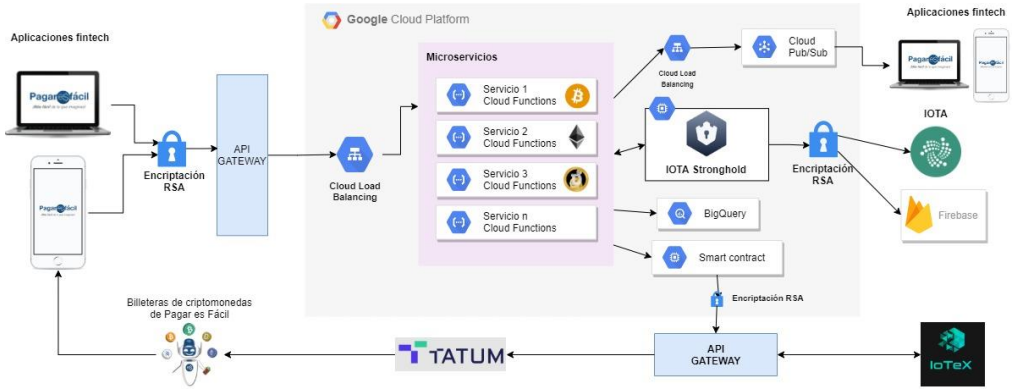

Figura 15: Arquitectura para marketplace usando smart contracts de Iotex

Fuente: Elaboración propia

Nro	Funcionalidades transaccionales	Propuesta de solución
1	Marketplace de productos/servicios	Smart contracts con Iotex y almacenamiento con Iota
2	Marketplace de criptomonedas	Smart contracts con Iotex, trading con Tatum y almacenamiento con Iota
3	Transferencia internas y externas de criptomonedas-	Trading con Tatum y almacenamiento con Iota
4	Link de pagos masivos	Almacenamiento de transacciones con Iota
5	Link de pagos por contacto	Almacenamiento de transacciones con Iota
6	Link de billetera	Almacenamiento de transacciones con Iota
7	Pagos recurrentes.	Almacenamiento de transacciones con Iota
8	Compra de saldos por Paypal.	Almacenamiento de transacciones con Iota
9	Compra de saldos por Red Activa	Almacenamiento de transacciones con Iota
10	Recarga de billetera con tarjetas de crédito	Almacenamiento de transacciones con Iota
11	Compra de giftcards	Almacenamiento de transacciones con Iota
12	Pago de servicios básicos	Almacenamiento de transacciones con Iota
13	Retiro de dinero	Almacenamiento de transacciones con Iota
14	Transferencias interbilleteras	Almacenamiento de transacciones con Iota
15	Remesas del exterior con tarjetas de crédito y billetera virtual	Almacenamiento de transacciones con Iota
16	Pagos con QR Code	Almacenamiento de transacciones con Iota
17	Api para desarrolladores y plugin de WordPress para WooCommerce	Almacenamiento de transacciones con Iota
18	Verificación de identidad	Almacenamiento de transacciones con Iota
19	Verificación de registro de tarjetas de crédito	Almacenamiento de transacciones con Iota
20	Compra de acciones	Almacenamiento de transacciones con Iota

Tabla 1: Funcionalidades transaccionales de Pagar es Fácil
Fuente: Datos estadísticos obtenidos de la plataforma.

CAPÍTULO II: MATERIALES Y MÉTODOS

2.1 Tipo de investigación seleccionada.

Dado a la revisión literaria y al planteamiento de aspectos como el problema, objetivo y variables de investigación realizado anteriormente, se determinó que esta investigación sea de tipo experimental y correlacional. Es de tipo experimental debido a que las variables de investigación serán manipuladas en un ambiente de producción con un grupo específico de sujetos obtenidos de las transacciones financieras realizadas por los usuarios de la aplicación de Pagar es Fácil para posteriormente verificar el comportamiento de los DLT ante distintas funcionalidades de la aplicación. En la tabla 2

Fase	Descripción	Aplicación
Baja transaccionalidad	Son aquellas transacciones que tomarán un tiempo en concatenarse a los DLT.	Se aplicarán en aquellas funcionalidades que requieran de la utilización de los smart contracts.
Alta transaccionalidad	Son aquellas transacciones que se concatenarán a los DLT ni bien termine la operación del usuario.	Se aplicarán en aquellas funcionalidades que requieran de la utilización de IOTA como almacenamiento.

Tabla 2: Fases de experimentación

Fuente: Elaboración propia.

Será una investigación de tipo correlacional debido a que se manipularán las variables para determinar la relación que existe entre la variable independiente, en este caso los DLT con la variable dependiente que es la ciberseguridad en aplicaciones Fintech y así obtener conclusiones que ayuden a responder al objetivo principal de esta investigación.

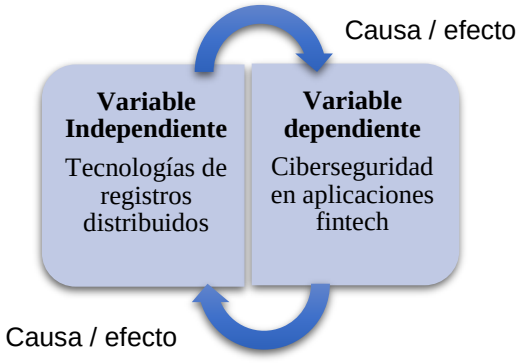

Figura 16: Causa/efecto de variables de investigación

Fuente: Elaboración propia.

2.2 Paradigma de investigación realizada.

Esta investigación se la realizó bajo un enfoque cuantitativo, siguiendo los pasos propuestos por Sampieri en su libro de metodología de la investigación científica (ver figura 17), tomando como métricas la latencia (tiempo de vida de los datos desde su envío hasta su recepción) y la cantidad de transacciones realizadas en la plataforma Pagar es Fácil. En la figura 18 se puede apreciar este enfoque cuantitativo desde un nivel arquitectónico.

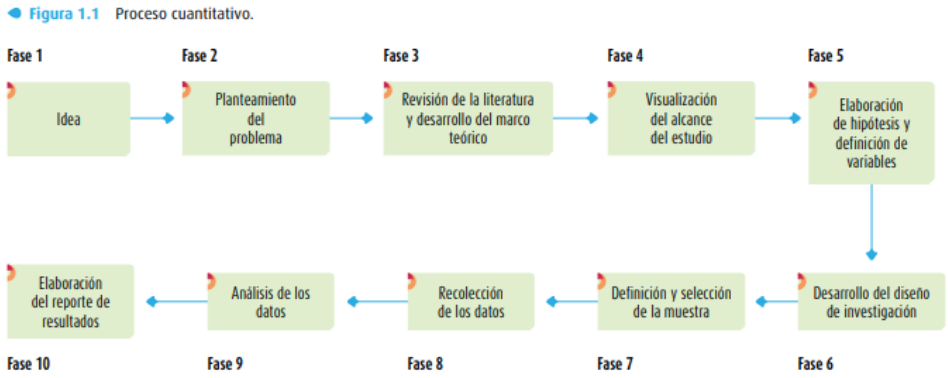

Figura 17: Fases del enfoque cuantitativo

Fuente: [149]

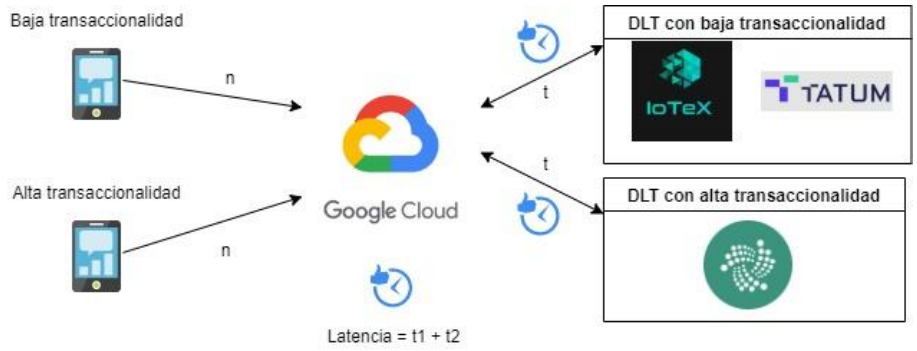

Figura 18: Enfoque cuantitativo a nivel arquitectónico

Fuente: Elaboración propia.

2.3 Población y muestra de la investigación.

La población con la cual se trabajará y analizará para la presente investigación serán todas las transacciones realizadas por los usuarios de Pagar es Fácil y debido a que tanto la cantidad de usuarios como las transacciones financieras incrementan día a día, se determinó que la población será infinita.

El tipo de muestreo será probabilístico debido a que no se puede seleccionar las transacciones de un usuario en específico debido a la gran cantidad de usuarios realizando transacciones al mismo tiempo, para eso se utilizará la fórmula de tamaño de muestra para poblaciones infinitas mostrado en la figura 19, en donde se estableció un nivel de confianza del 99% con su respectivo valor z-score de 2.576 y un margen de error de 5%, los resultados de la aplicación de la fórmula se muestran a continuación, siendo:

n= muestra = ?

p= probabilidad a favor = 50%

q= probabilidad en contra = 50%

z= nivel de confianza = 2.576 (99%)

e= error de muestra = 5%

$$n = \frac{z^2 * p * q}{e^2} = \frac{2.576^2 * 0.5 * 0.5}{0.05^2} = 664$$

Figura 19: Cálculo de la muestra

Fuente: Elaboración propia.

Dando como resultado un total de 664 transacciones que deberán ser analizadas para la comprobación de la hipótesis.

2.4 Método teórico utilizado.

El método teórico seleccionado para esta investigación fue el hipotético-deductivo, debido a que esta investigación plantea una hipótesis y las hipótesis son puntos de partida para nuevas deducciones entonces analizando los pasos que conlleva este método (observaciones, elaborar hipótesis, experimentación y refutación o verificación [150]) serán útiles para cumplir con el objetivo general de la investigación. La metodología propuesta por el método hipotético-deductivo quedó establecida de la siguiente manera:

Proceso del método hipotético-deductivo	
Observación	Detección de fraudes y estafas en las transacciones realizadas por usuarios de Pagar es Fácil.
Elaboración de hipótesis	La aplicación de tecnologías de registros distribuidos (DLT) incrementa la seguridad de los datos en el almacenamiento de las transacciones financieras en aplicaciones Fintech mitigando los casos de fraudes y estafas.
Deducción de consecuencias	Los casos de fraudes y estafas serán menores o nulos con la

	implementación de los DLT.
Experimentación	Se estudia la incidencia de una muestra obtenida de la población, en este caso las transacciones financieras, antes y después de la implementación de los DTL.
Refutación o verificación	Se muestran los resultados obtenidos y se comprueba o no la hipótesis planteada inicialmente.

Tabla 3: Proceso sistemático del método teórico utilizado

Fuente: Adaptado de [150]

2.5 Métodos empíricos utilizados.

2.6 Técnicas estadísticas utilizadas.

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] I. Foundation, «IOTA Smart Contracts Beta Release,» 2021. [En línea]. Available: https://blog.iota.org/iota-smart-contracts-beta-release/. [Último acceso: 21 10 2021].

[42] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi y K.-K. R. Choo, «A systematic literature review of blockchain cyber security,» *Digital Communications and Networks,* pp. 147-156, 2020.

[43] M. A. C. Y. D. Omar Ali, «The state of play of blockchain technology in the financial services sector: A systematic literature review,» *International Journal of Information Management,* vol. 54, 2020.

[44] S. Demirkan, I. Demirkan y A. McKee, «Blockchain technology in the future of business cyber security and accounting,» *Journal of Management Analytics,* vol. 7, nº 2, pp. 189-208, 2020.

[45] 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.

[46] 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].

[47] 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].

[48] K. Hausken, «Cyber resilience in firms, organizations and societies,» *Internet of Things,* vol. 11, 2020.

[49] A. M. Chitnis y J. M. Costa, «Videotex Services: Network and Terminal Alternatives,» *IEEE Transactions on Consumer Electronics,* Vols. %1 de %2CE-25, nº 3, pp. 269-278, 1979.

[50] L. Abdillah, «An Overview of Indonesian Fintech Application,» *The First International Conference on Communication, Information Technology and Youth Study (I-CITYS2019),* 2019.

[51] G. Bayramoğlu, «An Overview of the Artificial Intelligence Applications in Fintech and Regtech,» *he Impact of Artificial Intelligence on Governance, Economics and Finance,* vol. 1, p. 13, 2021.

[52] A. W. Ng y B. K. Kwok, «Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator,» *Journal of Financial Regulation and Compliance,* vol. 25, nº 4, pp. 422-434, 2017.

[53] R. KISHORE, M. AGRAWAL y H. R. RAO, «Determinants of Sourcing During Technology Growth and Maturity: An Empirical Study of e-Commerce Sourcing,» *Journal of Management Information Systems,* vol. 21, nº 3, pp. 47-82, 2014.

[54] M. Castro de Cifuentes, «Los contratos normativos y los contratos marco en el derecho privado contemporáneo,» *Revista Estudios Socio-Jurídicos,* vol. 21, nº 1, pp. 121-150, 2019.

[55] S. Nick, «Formalizing and Securing Relationships on Public Networks,» *First Monday,* 1997.

[56] M. Rahouti, K. Xiong y N. Ghani, «Bitcoin Concepts, Threats, and Machine-Learning Security Solutions,» *IEEE Access,* vol. 6, pp. 67189-67205, 2018.

[57] C. C. Vergara y L. F. Agudo, «Fintech and Sustainability: Do They Affect Each Other?,» *Sustainability,* vol. 13, nº 13, p. 7012, 2021.

[58] M. Xu, X. Chen y G. Kou, «A systematic review of blockchain,» *Financial Innovation,* vol. 5, nº 27, 2019.

[59] R. Colomo-Palacios, M. Sánchez-Gordón y D. Arias-Aranda, «A critical review on blockchain assessment initiatives: Atechnology evolution viewpoint,» *Journal of Software: Evolution and Process,* 2020.

[60] S. Bistarelli, G. Mazzante, M. Micheletti, L. Mostarda, D. Sestili y F. Tiezzi, «Ethereum smart contracts: Analysis and statistics of their source code and opcodes,» *Internet of Things,* vol. 11, 2020,.

[61] A. L. Vivar, A. L. Sandoval, O. L. Javier y G. Villalba, «A security framework for Ethereum smart contracts,» *Computer communications,* vol. 175, nº 15, pp. 119-129, 2021.

[6 2] M. U. Chowdhury, K. Suchana, S. M. E. Alam y M. M. Khan, «Blockchain Application in Banking,» *Journal of Software Engineering,* vol. 14, pp. 298-311, 2021.

[6 3] M. Mazzoni, A. Corradi y V. D. Nicola, «Performance evaluation of permissioned blockchains for financial applications: The ConsenSys Quorum case study,» *Blockchain: Research and Applications,* 2021.

[6 4] A. I. Sanka, M. Irfan y R. C. C. Ian Huang, «A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research,» *Computer Communications,* vol. 169, 2021.

[6 5] J. Polge, J. Robert y Y. L. Traon, «Permissioned blockchain frameworks in the industry: A comparison,» *ICT Express,* vol. 7, nº 2, pp. 229-233, 2021.

[6 6] J. J. R. Yasay, «The Dawn of Digital Coins: A Literature Review on Cryptocurrency in the Philippines,» *International Journal of Innovative Science and Research Technology,* vol. 6, nº 5, 2021.

[6 7] S. Perera, S. Nanayakkara, M. Rodrigo, S. Senaratne y R. Weinand, «Blockchain technology - Is it hype or real in the construction industry,» *Journal of Industrial Information Integration,* vol. 17, 2020.

[6 8] E. Silva, X. Huang y H. Hassani, «Banking with blockchain-ed big data,» *Journal of Management Analytics,* vol. 5, nº 4, pp. 256-275, 2018.

[6 9] S. Wan, M. Li, G. Liu y C. Wang, «Recent advances in consensus protocols for blockchain: a survey,» *Wireless Networks,* vol. 26, p. 5579–5593, 2020.

[7 0] J. Duan, C. Zhang, Y. Gong, S. Brown y Z. Li, «A Content-Analysis Based Literature Review in Blockchain Adoption within Food Supply Chain,» *International Journal of Environmental Research and Public Health,* vol. 17, nº 5, 2020.

[7 1] D. F. Maesa, «Blockchain 3.0 applications survey,» *Journal of Parallel and Distributed Computing,* vol. 138, pp. 99-114, 2020.

[7 2] Johar, S. a. Ahmad, N. a. Asher, W. a. Cruickshank, H. a. Durrani y Amad, «Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey,» *Applied Sciences,* vol. 11, nº 14, 2021.

[7 3] U. Sarfraz, M. Alam, S. Zeadally y A. Khan, «Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions,» *Computer Networks,* Vols. %1 de %2148,, pp. 361-372, 2019.

[7 4] A. Shahaab, B. Lidgey, C. Hewage y I. Khan, «Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review,» *IEEE Access,* vol. 7, pp. 43622-43636, 2019.

[75] M. Salimitari, M. Chatterjee y Y. P. Fallah, «A survey on consensus methods in blockchain for resource-constrained IoT networks,» *Internet of Things,* vol. 11, 2020.

[76] B. Bhushan, C. Sahoo, P. Sinha y A. Khamparia, «Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions,» *Wireless Networks,* vol. 27, p. 55–90, 2021.

[77] U. Majeed, L. U. Khan, I. Yaqoob, S. A. Kazmi, K. Salah y C. S. Hong, «Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges,» *Journal of Network and Computer Applications,* vol. 181, 2021.

[78] Z. Wang, H. Jin, W. Dai, K.-K. R. Choo y D. Zou, «Ethereum smart contract security research: survey and future research opportunities,» *Frontiers of Computer Science,* vol. 15, nº 152802, 2021.

[79] A. Daragmeh, C. Lentner y J. Sági, «FinTech payments in the era of COVID-19: Factors influencing behavioral intentions of "Generation X" in Hungary to use mobile payment,» *Journal of Behavioral and Experimental Finance,* vol. 32, 2021.

[80] J. Chigada y R. Madzinga, «Cyberattacks and threats during COVID-19: A systematic literature review,» *South African Journal of Information Management,* vol. 23, pp. 1 - 11, 2021.

[81] G. Iakovakis, C.-G. Xarhoulacos, K. Giovas y D. Gritzalis, «Analysis and Classification of Mitigation Tools against Cyberattacks in COVID-19 Era,» *Security and Communication Networks,* vol. 2021, 2021.

[82] A. Mihailović y N. Rašović, «Cybersecurity in the New Reality - Systematic Review in the context of covid 19,» *International Journal of Innovative Science and Research Technology,* vol. 5, nº 12, 2020.

[83] A. R.O., C. M. y F. W, «Cybersecurity Attacks During COVID-19: An Analysis of the Behavior of the Human Factors and a Proposal of Hardening Strategies,» *Advances in Cybersecurity Management,* 2021.

[84] M. Hijji y G. Alam, «A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions,» *IEEE Access,* vol. 9, pp. 7152-7169, 2021.

[85] J. Angelis y E. R. d. Silva, «Blockchain adoption: A value driver perspective,» *Business Horizons,* vol. 62, nº 3, pp. 307-314, 2019.

[86] B. K. Mohanta, D. Jena, U. Satapathy y S. Patnaik, «Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology,» *Internet of Things,* vol. 11, 2020.

[87] U. Bodkhe, «Blockchain for Industry 4.0: A Comprehensive Review,» *IEEE Access,* vol. 8, pp. 79764-79800, 2020.

[88] B. Gutiérrez-Nieto y C. Serrano-Cinca, «20 years of research in microfinance: An information management approach,» *International Journal of Information Management,* vol. 47, pp. 183-197, 2019.

[89] J. R. A. Yupanqui y S. B. Oré, «Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento,» *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação,* nº 25, 2017.

[90] M. Younas, D. N. Jawawi, I. Ghani, T. Fries y R. Kazmi, «Agile development in the cloud computing environment: A systematic review,» *Information and Software Technology,* vol. 103, pp. 142-158, 2018.

[91] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan y K.-K. R. Choo, «Blockchain-based identity management systems: A review,» *Journal of Network and Computer Applications,* vol. 166, 2020.

[92] D. Sheng, L. Ding, B. Zhong, P. E. Love, H. Luo y J. Chen, «Construction quality information management with blockchains,» *Automation in Construction,* vol. 120, 2020.

[93] A. Perdana, A. Robb, V. Balachandran y F. Rohde, «Distributed ledger technology: Its evolutionary path and the road ahead,» *Information & Management,* vol. 58, nº 3, 2021.

[94] L. Hashimy, H. Treiblmaier y G. Jain, «Distributed ledger technology as a catalyst for open innovation adoption among small and medium-sized enterprises,» *The Journal of High Technology Management Research,* vol. 32, nº 1, 2021.

[95] P. Zhuang, T. Zamir y H. Liang, «Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey,» *IEEE Transactions on Industrial Informatics,* vol. 17, nº 1, pp. 3-19, 2021.

[96] G. S. Sadasiuvam, «A critical review on using blockchain technology in education domain,» *Handbook of Deep Learning in Biomedical Engineering,* pp. 85-121, 2021.

[97] B. Farahani, F. Firouzi y M. Luecking, «The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions,» *Journal of Network and Computer Applications,* vol. 177, 2021.

[98] A. I. Sanka y R. C. Cheung, «A systematic review of blockchain scalability: Issues, solutions, analysis and future research,» *Journal of Network and Computer Applications,* vol. 195, 2021.

[99] X. Fu, H. Wang y P. Shi, «A survey of Blockchain consensus algorithms: mechanism, design and applications,» *Science China Information Sciences,* vol. 64, 2021.

[100] M. A. Jan, J. Cai, X.-C. Gao, F. Khan, S. Mastorakis, M. Usman, M. Alazab y P. Watters, «Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions,» *Journal of Network and Computer Applications,* vol. 175, 2021.

[101] Y. Lu, «The blockchain: State-of-the-art and research challenges,» *Journal of Industrial Information Integration,* pp. 80-90, 2019.

[102] Q. Feng, D. He, S. Zeadally, M. K. Khan y N. Kumar, «A survey on privacy protection in blockchain system,» *Journal of Network and Computer Applications,* vol. 126, pp. 45-58, 2019.

[103] H. -N. Dai, Z. Zheng y Y. Zhang, «Blockchain for Internet of Things: A Survey,» *IEEE Internet of Things Journal,* vol. 6, nº 5, pp. 8076-8094, 2019.

[104] G. Sargsyan, N. Castellon, R. Binnendijk y P. Cozijnsen, «Blockchain Security by Design Framework for Trust and Adoption in IoT Environment,» *2019 IEEE World Congress on Services (SERVICES),* pp. 15-20, 2019.

[105] R. Yang, R. Wakefield, S. Lyu, S. Jayasuriya, F. Han, X. Yi, X. Yang, G. Amarasinghe y S. Chen, «Public and private blockchain in construction business process and information integration,» *Automation in Construction,* vol. 118, 2020.

[106] A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi y A. S. A.-M. AL-Ghamdi, «Blockchain Platforms and Access Control Classification for IoT Systems,» *Symmetry,* vol. 12, nº 10, 2020.

[107] D. C. Nguyen, P. N. Pathirana, M. Ding y A. Seneviratne, «Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges,» *IEEE Communications Surveys & Tutorials,* vol. 22, nº 4, pp. 2521-2549, 2020.

[108] X. Fan y Q. Chai, «Roll-DPoS: A Randomized Delegated Proof of Stake Scheme for Scalable Blockchain-Based Internet of Things Systems,» *In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous '18),* 2018.

[109] A. Pieroni, N. Scarpato y L. Felli, «Blockchain and IoT Convergence—A Systematic Survey on Technologies, Protocols and Security,» *Applied Sciences,* vol. 10, nº 19, 2020.

[110] C. Laneve y C. S. Coen, «Analysis of smart contracts balances,» *Blockchain: Research and Applications,* 2021.

[111] N. Khan, B. Kchouri, N. A. Yatoo, Z. Kräussl, A. Patel y R. State, «Tokenization of sukuk: Ethereum case study,» *Global Finance Journal,* 2020.

[12] Tatum, «Welcome to Tatum,» 2021. [En línea]. Available: https://docs.tatum.io/. [Último acceso: 02 11 2021].

[13] Tatum, «Supported Blockchains,» 2021. [En línea]. Available: https://docs.tatum.io/supported-blockchains. [Último acceso: 02 11 2021].

[14] Tatum, «Arquitectura de Tatum,» 2021. [En línea]. Available: https://docs.tatum.io/tatum-architecture. [Último acceso: 02 11 2021].

[15] S. Sengupta, C.-F. Chiang, B. Andriamanalimanana, J. Novillo y A. Tekeoglu, «A Hybrid Adaptive Transaction Injection Protocol and Its Optimization for Verification-Based Decentralized System,» *Future Internet,* vol. 11, nº 8, 2019.

[16] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues y K. Ko, «Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues,» *IEEE Access,* vol. 6, pp. 1513-1524, 2018.

[17] J. Sengupta, S. Ruj y S. D. Bit, «A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT,» *Journal of Network and Computer Applications,* vol. 149, 2020.

[18] S. Popov, «IOTA: Feeless and Free,» *IEEE Blockchain Technical Briefs,* 2019.

[19] A. Panarello, N. Tapas, G. Merlino, F. Longo y A. Puliafito, «Blockchain and IoT Integration: A Systematic Survey,» *Sensors,* vol. 18, nº 8, 2018.

[20] I. Foundation, «The Coordicide,» 2019. [En línea]. Available: https://files.iota.org/papers/20200120_Coordicide_WP.pdf.

[21] J. H. Khor, M. Sidorov y P. Y. Woon, «Public Blockchains for Resource-Constrained IoT Devices—A State-of-the-Art Survey,» *IEEE Internet of Things Journal,* vol. 8, nº 15, pp. 11960-11982, 2021.

[22] I. Foundation, «The new Chrysalis Network is Live!,» IOTA, 2021. [En línea]. Available: https://blog.iota.org/the-new-chrysalis-network-is-live/. [Último acceso: 2021].

[23] S. Popov y W. Buchanan, «FPC-BI: Fast Probabilistic Consensus within Byzantine Infrastructures,» *arXiv,* 2021.

[1 U. A. M. R. S. a. M. M. Y. S. H. Bhaharin, «Issues and Trends in Information
24 Security Policy Compliance,» *6th International Conference on Research and*
] *Innovation in Information Systems (ICRIIS)*, pp. 1-6, 2019.

[1 E. A. Kirillova, U. M. Yakhutlov, X. Wenqi, G. Huiting y W. Suyu, «Information
25 Security in the Management of Personnel in a Modern Organization,» *2020*
] *International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, pp. 107-109, 2020.

[1 S. V. Aleksandrova, V. A. Vasiliev y M. N. Aleksandrov, «Problems of
26 Implementing Information Security Management Systems,» *2020 International*
] *Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, pp. 78-81, 2020.

[1 Y. Wang, J. Yao y X. Yu, «Information Security Protection in Software Testing,»
27 *2018 14th International Conference on Computational Intelligence and Security*
] *(CIS)*, pp. 449-452, 2018.

[1 N. Shariffuddin y A. Mohamed, «IT Security and IT Governance Alignment: A
28 Review,» *In Proceedings of the 3rd International Conference on Networking,*
] *Information Systems & Security (NISS2020)*, pp. 1-8, 2020.

[1 S. S. Tirumala, M. R. Valluri y G. Babu, «A survey on cybersecurity awareness
29 concerns, practices and conceptual measures,» *2019 International Conference on*
] *Computer Communication and Informatics (ICCCI)*, pp. 1-6, 2019.

[1 Y. Lu y L. D. Xu, «Internet of Things (IoT) Cybersecurity Research: A Review of
30 Current Research Topics,» *IEEE Internet of Things Journal*, vol. 6, nº 2, pp. 2103-
] 2115, 2019.

[1 Z. Wang, L. Sun y H. Zhu, «Defining Social Engineering in Cybersecurity,» *IEEE*
31 *Access*, vol. 20, pp. 85094-85115, 2020.
]

[1 M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb y S. Mahmood, «Cyber Security
32 Threats and Vulnerabilities: A Systematic Mapping Study,» *Arabian Journal for*
] *Science and Engineering*, vol. 45, p. 3171–3189, 2020.

[1 A. Tundis, W. Mazurczyk y M. Mühlhäuser, «A review of network vulnerabilities
33 scanning tools: types, capabilities and functioning,» *In Proceedings of the 13th*
] *International Conference on Availability, Reliability and Security (ARES 2018)*, p. 1–10, 2018.

[1 R. Kumar y R. Goyal, «On cloud security requirements, threats, vulnerabilities and
34 countermeasures: A survey,» *Computer Science Review*, vol. 33, pp. 1-48, 2019.
]

[1 N. X. a. J. R. P. Yang, «Data Security and Privacy Protection for Cloud Storage: A
35 Survey,» *IEEE Access,* vol. 8, pp. 131723-131740, 2020.
]

[1 M. Majid y P. Luo, «Forty years of attacks on the RSA cryptosystem: A brief
36 survey,» *Journal of Discrete Mathematical Sciences and Cryptography,* pp. 9-29,
] 2019.

[1 P. Kumar y S. B. Rana, «Development of modified AES algorithm for data
37 security,» *Optik,,* vol. 127, nº 4, pp. 2341-2345, 2016.
]

[1 M. D. Hire, M. Bhatt, M. Anand y C. Harde, «Literature Survey of Two-Way
38 Authentication System,» *International Journal of Scientific Research &*
] *Engineering Trends,* vol. 7, nº 2, 2021.

[1 E. Huseynov y J.-M. Seigneur, «Chapter 50 - Context-Aware Multifactor
39 Authentication Survey,» *Computer and Information Security Handbook (Third*
] *Edition),* pp. 715-726, 2017.

[1 K. F. Steinmetz, A. Pimentel y W. R. Goe, «Performing social engineering: A
40 qualitative study of information security deceptions,» *Computers in Human*
] *Behavior,* vol. 124, 2021.

[1 J. Li y L. Zhang, «Sender dynamic, non-repudiable, privacy-preserving and strong
41 secure group communication protocol,» *Information Sciences,* vol. 414, pp. 187-
] 202, 2017.

[1 B. L. y G. M., Microservices: The Evolution and Extinction of Web Services?,
42 Springer, Cham, 2020.
]

[1 H. Chen, M. Pendleton, L. Njilla y S. Xu, «A Survey on Ethereum Systems
43 Security: Vulnerabilities, Attacks, and Defenses,» *ACM Computing Surveys,* vol.
] 53, nº 3, p. 1–43, 2020.

[1 I. Sadgali, N. Sael y F. Benabbou, «Detection of credit card fraud: State of art,»
44 *IJCSNS International Journal of Computer Science and Network Security,* vol. 18,
] nº 11, 2018.

[1 M. Saraswat y R. C. Tripathi, «Cloud Computing: Analysis of Top 5 CSPs in SaaS,
45 PaaS and IaaS Platforms,» *2020 9th International Conference System Modeling and*
] *Advancement in Research Trends (SMART),* pp. 300-305, 2020.

[1 S. Yulianto, C. Lim y B. Soewito, «Information security maturity model: A best
46 practice driven approach to PCI DSS compliance,» *2016 IEEE Region 10*
] *Symposium (TENSYMP),* pp. 65-70, 2016.

[147] PEF, «Presentación de negocios 2021 de Pagar es Fácil,» 2021. [En línea]. Available: https://firebasestorage.googleapis.com/v0/b/backservicespagos.appspot.com/o/presentaciones%2FPRESENTACIO%CC%81N%20DE%20NEGOCIOS%202021%20-ECUADOR-.pdf?alt=media&token=464dd77e-cebb-4fa0-9bad-9c8d946040bb. [Último acceso: 27 10 2021].

[148] PEF, «Quienes somos - Pagar es Fácil,» 2021. [En línea]. Available: https://www.pagaresfacil.com/quienes-somos-pagar-es-facil. [Último acceso: 27 10 2021].

[149] R. Sampieri, Metodología de la investigación, México: McGraw Hill, 2014.

[150] A. Rodríguez Jiménez y A. O. Pérez Jacinto, «Métodos científicos de indagación y de construcción del conocimiento,» *Revista Escuela de Administración de Negocios*, nº 82, pp. 1-26, 2017.