UNIVERSIDAD TÉCNICA DE MACHALA

Maestría en Software

Asignatura:

Titulación II

Tema:

Taller N° 5: Estructura del Trabajo de Titulación-Escritura del Marco Teórico

Docente:

Walter Fuertes Díaz, PhD

Estudiante:

Ing. Jimmy Fernando Castillo Crespín

2021-2022

CAPÍTULO I: ESTADO DE ARTE

El presente capítulo está destinado a la elaboración del estado de arte, el cual está compuesta por los antecedentes históricos, antecedentes conceptuales y finalmente los antecedentes contextuales. Para el desarrollo del mismo, se ha realizado una revisión sistemática de literatura (SLR) tomando en cuenta el procedimiento de la guía metodológica propuesta por Barbara Kitchenham [51].

1.1 Preguntas de investigación.

Se elaboraron las siguientes preguntas para la búsqueda de información acerca de las tecnologías de registros distribuidos y su aplicación en las aplicaciones Fintech, la tabla 1 detalla el resultado de las preguntas y dimensiones seleccionadas.

Preguntas	Dimensiones
¿Qué tecnologías de registros distribuidos se han aplicado en las Fintech para disminuir casos de delitos informáticos?	Técnicas DLT, implementaciones de DLT en Fintech, delitos informáticos
¿Cómo se implementa la metodología ABCDE en conjunto con una arquitectura de microservicios en Google Cloud para el desarrollo de sistemas Dapps?	Metododología ABCDE, microservicios cloud.
¿Cómo se implementa microservicios para registros transaccionales de coste cero con IOTA Tangle e identidad digital mediante verificación biométrica y NFT con Tatum para incrementar la probabilidad de ganar disputas financieras en casos de fraudes en transacciones financieras?	IOTA Tangle, identidad digital con NFT, Tatum.
¿Cómo se implementa smarts contracts en microservicios con IOTEX blockchain para disminuir el porcentaje de casos de estafas en transacciones financieras?	Smarts contracts, IOTEX blockchain.

Tabla 1: Preguntas de investigación para el SLR

Fuente: *Elaboración propia*

1.2 Proceso de búsqueda.

Dentro del proceso de búsqueda, se seleccionaron las siguientes bases de datos propuestas por el instructivo de titulación de la maestría:

- IEEE Xplore
- Science Direct
- Taylor and Francis.
- Springer

1.3 Criterios de inclusión y exclusión.

Dentro de los criterios de exclusión se consideraron los siguientes parámetros:

- Estudios duplicados.
- Estudios que no se incluyeron en las bases de datos de selección.
- Resultados de libros, cursos-

Dentro de los criterios de inclusión se consideraron los siguientes parámetros:

- Solo estudios primarios.
- Solo investigaciones con resultados.
- Escritos en inglés y español.
- Estudios de los últimos 5 años.
- Estudios de aplicación de DLT en aplicaciones financieras o Fintech.
- Deben ser journals o conference paper.
- Temas principales: DLT y ciberseguridad.

1.4 Cadena de búsqueda.

La cadena de búsqueda se elaboró en base a las preguntas de investigación y se tomó en cuenta operadores lógicos como AND y OR y se seleccionó filtrando por aspectos como el título, palabras claves, metadatos etc, quedando de la siguiente manera:

"Cybersecurity in Fintech" and ("Distributed Ledger Technologies" or "Blockchain" or "Tangle" or "Smart Contracts" or "IOTA" or "IOTEX")

1.5 Selección de estudios y fase de revisión.

Para la selección de estudios se usó las bases de datos y cadena de búsqueda previamente seleccionadas y formada, la tabla 2 muestra el resultado de este proceso.

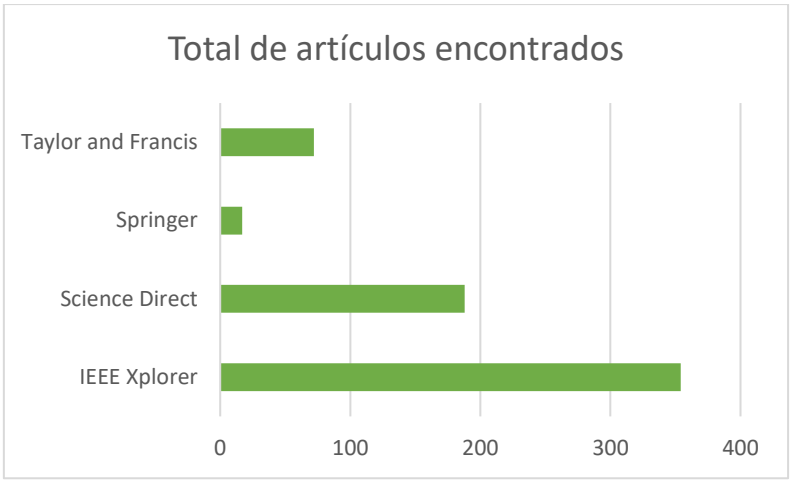
Bases de datos	Total de artículos encontrados
IEEE Xplorer	354
Science Direct	188
Springer	17
Taylor and Francis	72

Total	631

Tabla 2: Total de artículos encontrados

Fuente: *Elaboración propia*

En base a la tabla anterior se realizó el siguiente cuadro estadístico.



Fuente: *Elaboración propia*

En base al total de artículos encontrados en las diferentes bases de datos científicas, se realizó la fase de revisión partiendo del total de artículos, seguido de los filtrados de remover artículos duplicados, leer abstracts y títulos, aplicar criterios de exclusión e inclusión y finalmente leer el texto completo, la tabla 3 muestra el resultado de esta fase de revisión.

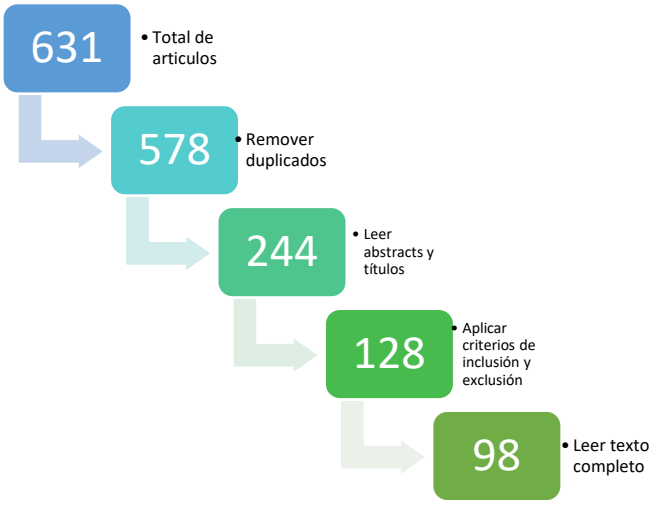


Tabla 3: Fase de revisión del SLR

Fuente: *Elaboración propia*

1.6 Presentación de resultados.

El resultado del SLR desarrollado se encuentra disponible en el Anexo 1, donde se detalla los 98 artículos científicos seleccionados para la elaboración de los antecedentes históricos, conceptuales y contextuales que se presentan a continuación.

1.7 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 [52], uno de los primeros sistemas e-commerce que implementaron las ventas online [53] surgiendo desde este momento el término Fintech 1.0 [54].

Seguidamente por los años 90 con la aparición de las primeras aplicaciones Fintech como Paypal 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 [55]. Pero a su vez, el número de estafas, fraudes y robo de información incrementaron en diversas formas por parte de hackers que aún siguen presentes en tiempos actuales tal y como lo detallan los autores [56], [14] y [15].

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 [57], 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 [58].

Desde los años 90 hasta la actualidad, 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 [59]. Pero esta situación se volvió viable en el año 2009 con la aparición del bitcoin por Satoshi Nakamoto [60] 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, que son empresas emergentes cuya característica principal es tener proyectos de rápido crecimiento y vertiginoso [61] 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 [62].

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) [62] [63], todas estas nuevas funcionalidades son prácticas para dar solución a posibles delitos informáticos 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 [64]). 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 [65] y este aspecto es conveniente para ser utilizada en compras por internet de un marketplace por citar un ejemplo práctico.

Debido a estos avances del blockchain, fue a partir del año 2015 que entidades financieras decidieran invertir en la infraestructura blockchain. Entre las entidades más destacadas se encuentran: J.P Morgan Chase que creó una división enfocada enteramente al blockchain [66] de las cuales se obtuvieron como resultado su propia blockchain privada denominada Quorum desarrollado bajo el código Ethereum [67] y en el año 2019 lanzaron su propia criptomoneda llamada JPMCoin [68]. Cabe recalcar que Quorum fue diseñado para satisfacer las necesidades de las instituciones financieras [69].

Otros casos significativos 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 [70]) para desarrollar servicios de pagos internacionales dando como resultado su servicio Fintech denominado Santander One Pay FX [71]; el banco 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 [72].

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 [26]. 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) [73] lo que quiere decir que, mientras más crezca la red, mayor será el tiempo de procesar una transacción y esto ya no es tan rentable para aplicaciones desarrolladas por startups.

De igual forma sucede con las comisiones que se cobran por cada transacción en blockchain. Estas comisiones no están reguladas y varían dependiendo de varios factores como el congestionamiento de la red, el valor de la criptomoneda [74] 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 [14], [15], [26], [27] & [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 rendimiento 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 (Dapps) pero con la ventaja de tener mayor capacidad que las redes pioneras del blockchain (bitcoin y Ethereum) [75] , un producto de esta nueva tecnología es la red Cardano (criptomoneda ADA) [76].

Sin embargo, aunque estas nuevas redes que surgieron del blockchain 3.0 solucionan gran parte de los problemas ocasionados por la blockchain 1.0 y 2.0, aún siguen sin mitigarlas del todo, dando nacimiento al 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) [77].

Gracias al protocolo de consenso de IOTA, llamado FPC (Fast Probabilistics Consensus) [78], 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 [79], haciéndolo perfecto para ser utilizado en micropagos de IoT [80] o para aplicaciones Fintech.

En cuestión de la rentabilidad, IOTA no 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 [81]. La ventaja de esto es que incrementa la rentabilidad en las transacciones realizadas en cualquier aplicación, en aspectos como velocidad, seguridad y escalabilidad.

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 [43], los smart contract se encuentra actualmente en fase beta para los desarrolladores. Por lo tanto, Ethereum y Cardano son los más utilizados actualmente en la construcción de smart contracts [82].

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 [83], pero a su vez se detectaron un incremento de la ciberdelincuencia en estas aplicaciones [84], [85], [86], [87] & [88].

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 todos los delitos informáticos 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 [89] & Mohanta y otros [90].

Actualmente se está trabajando en la blockchain 4.0 en conjunto con la industria 4.0, que a pesar que en esta investigación no se utilizará esta tendencia, la característica de inclusión de la inteligencia artificial al blockchain [91] sería un gran avance para la mitigación de fraudes y estafas en transacciones financieras online. La figura 1 ilustra una síntesis de los antecedentes históricos elaborado para esta investigación.

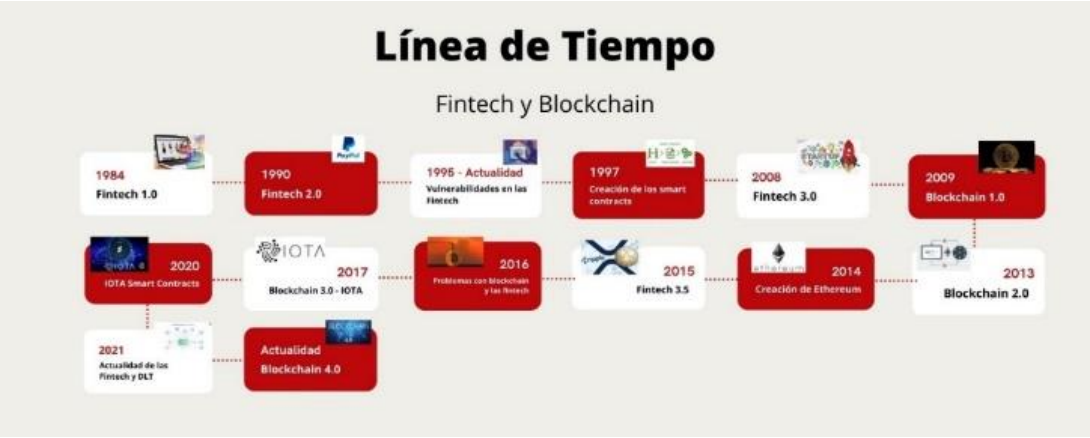


Figura 1: Organización cronológica de los antecedentes de las fintech y blockchain.
Fuente: Elaboración propia

1.8 Antecedentes conceptuales.

1.8.1 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 implementación de tecnologías de registros distribuidos (DLT) en una arquitectura de microservicios cloud disminuye casos de estafas y fraudes en transacciones financieras de una aplicación Fintech.

Ho: La implementación de tecnologías de registros distribuidos (DLT) en una arquitectura de microservicios cloud no disminuye casos de estafas y fraudes en transacciones financieras de una aplicación Fintech.

1.8.2 Red de categorías de las variables.

1.8.2.1 Variable independiente.

- Tecnologías de registros distribuidos (DLT) en microservicios cloud.

1.8.2.2 Variable dependiente.

- Delitos informáticos (estafas y fraudes) en aplicaciones Fintech.

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

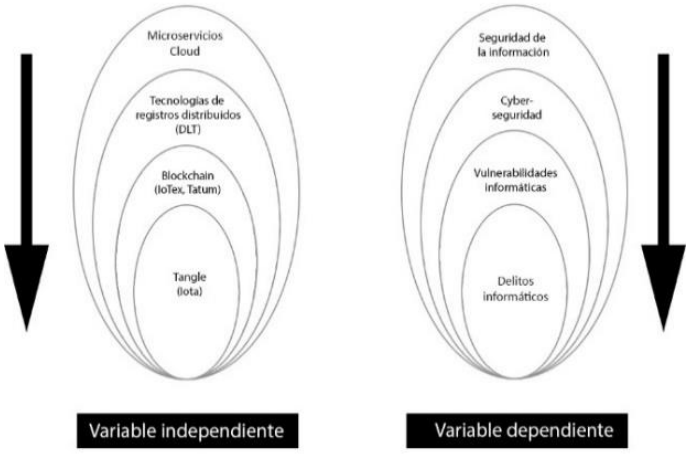


Figura 2: Variables dependientes e independientes seleccionadas

Fuente: Elaboración propia

1.8.3 Fundamentación teórica de la variable independiente.

Las tecnologías de registros distribuidos en microservicios cloud 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 son los microservicios cloud a lo más específico que son las tecnologías de registros distribuidos.

1.8.3.1 Microservicios cloud.

Las arquitecturas de microservicios implementadas en cloud computing son actualmente una de las tendencias más utilizadas para el desarrollo de software complejas y distribuidas debido a su potencial de escalabilidad y seguridad para la información [92], esta afirmación viene fundamentada por los autores Hannousse & Yahiouche en su artículo [93] donde concluyeron que los microservicios nacieron con la finalidad de enfrentar la escalabilidad horizontal y vertical y los mantenimientos de los mismos mediante la utilización de patrones de diseños arquitectónicos.

Sin embargo, las vulnerabilidades en sistemas basados en microservicios en aspectos como el no repudio, integridad y confidencialidad han aumentado [94], surgiendo los DLT como una nueva forma de protección para la información, esta afirmación acerca de los DLT viene sustentada por los trabajos realizados por Yang [95] y Sheng [96].

1.8.3.1.1 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 descentralizada, proporcionando la ventaja de aumentar de seguridad de los datos [97], 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.

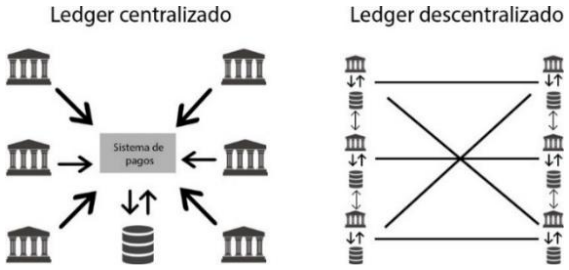


Figura 3: Ledger centralizado y descentralizado en un ambiente Fintech

Fuente: Elaboración propia

Entre las ventajas de los DLT, el autor Hashimy [98] detalla 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 [99] 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 [100] 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.

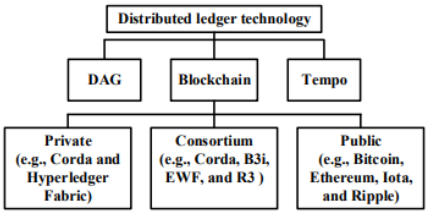


Figura 4: Clasificación de los DLT

Fuente: *[99]*

En la figura 5 elaborado por Bahar [101] 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).

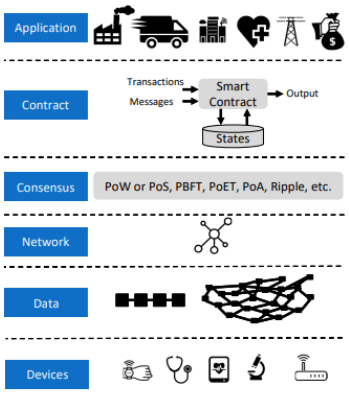


Fig. 2: DLT Stack.

Figura 5: Características de los DLT

Fuente: *[101]*

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 [102] 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) [103] y también ventajas únicas como la implementación de smart contracts muy baratas con IoTex blockchain [44] o un almacenamiento con coste cero con IOTA [40].

1.8.3.1.2 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 [104]. El autor Feng [105] 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 la 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 [106].

1.8.3.1.2.1 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 [107] y [108] 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.

1.8.3.1.2.2 Ventajas del blockchain.

El autor Abdi & otros [109] 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.

1.8.3.1.2.3 Plataformas blockchain

Yang [108] y Nguyen [110] mencionan varias plataformas blockchain como:

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

1.8.3.1.2.4 IoTex.

IoTex es una infraestructura de blockchain cuya principal característica es su protocolo de consenso en tiempo real llamado Roll-DPoS [111] que 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 [112].

Gracias al protocolo Roll-DPoS se obtiene una red con un rendimiento significativamente más alta y de costo menor por cada transacción en comparación a otras blockchain [44], 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 implementado con IoTex blockchain.

1.8.3.1.2.5 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 [113].

1.8.3.1.2.6 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 [114].

1.8.3.1.2.7 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" [115]. Tatum admite las siguientes redes de blockchain para su desarrollo e implementación [116]:

- 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 [117], brinda beneficios como facilidad de utilizar sus apis, prueba del futuro y escalabilidad en el desarrollo de aplicaciones.

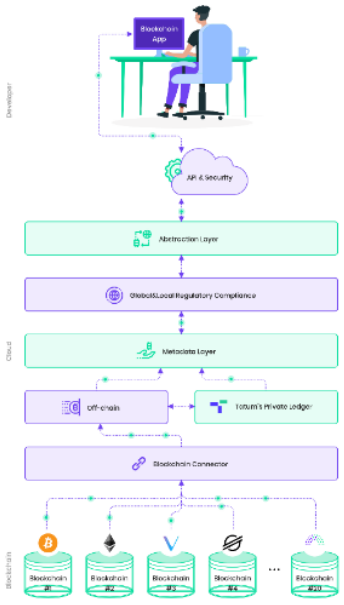


Figura 6: Arquitectura de Tatum

Fuente: [117]

1.8.3.1.3 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) [118] 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 [119], en la figura 8 se muestra gráficamente la diferencia entre la arquitectura blockchain y Tangle.

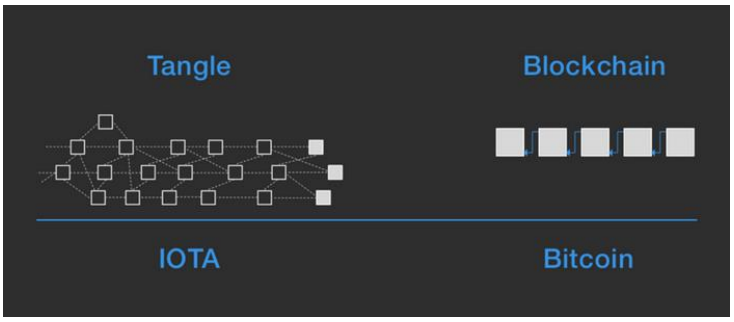


Figura 7: Arquitectura Blockchain vs Tangle

Fuente: *Elaboración propia.*

El funcionamiento de Tangle 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 [120].

Entre las ventajas que ofrece Tangle, los autores [118], [119] & [120] 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.

1.8.3.1.3.1 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, costo cero en comisiones y descentralización. Estas ventajas son posibles gracias al protocolo de

conseso Fast Probabilistic Consensus (FPC), el cual según Popov & Buchanan lo definen como un “protocolo de consenso binario probabilísticos el cual no posee líder, de baja complejidad comunicacional, convirtiéndolo en una tecnología robusta” [121].

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 [122]. Su principal objetivo es la seguridad durante el flujo de la información en especial para el ambiente Iot [123].

Uno de los inconvenientes con Iota es que no es totalmente descentralizada, cuenta con un nodo origen llamado coordinador que se encarga principalmente de evitar ataques de red [124] [125] pero esto se quiere solucionar con el nuevo protocolo conocido como chrysalis con la salida de IOTA 2.0 nectar reléase [126].

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 [43] dando un gran paso sobre esta arquitectura.

1.8.3.1.3.2 IOTA Stronghold

Librería open-source escrita en Rust que utiliza una base de datos segura para proteger cualquier secreto digital de posibles hackers, como contraseñas, privates key etc y estas nunca sean revelados [127]. Gracias a esta librería, aumentaría la seguridad al momento de trabajar con contraseñas, llaves privadas o información sensible generadas en transacciones financieras Fintech.

1.8.4 Fundamentación teórica de la variable dependiente.

1.8.4.1 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 [128].

El objetivo principal de los S.I, según los autores Kirillova & otros [129] 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 [130].

La detección de riesgos por lo general se los realiza en un ambiente de pruebas, el autor Wang [131] 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.

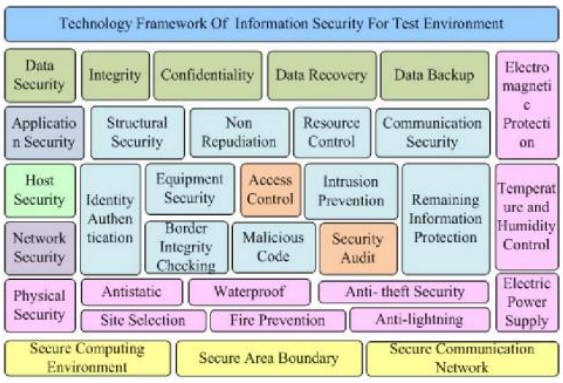


Figura 8: Framework de seguridad de la información para ambientes de pruebas

Fuente: *[131]*

1.8.4.2 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 [132].

Sin embargo, el autor Tirumala [133] 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 del software, los ataques informáticos siguen ocurriendo debido al aumento de las personas en utilizar dispositivos conectados a internet [134] y a la creatividad de los atacantes en utilizar la ingeniería social para penetrar sistemas [135].

1.8.4.3 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 [136]. Estas vulnerabilidades son explotadas por hackers 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 [137], 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 [138] 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.

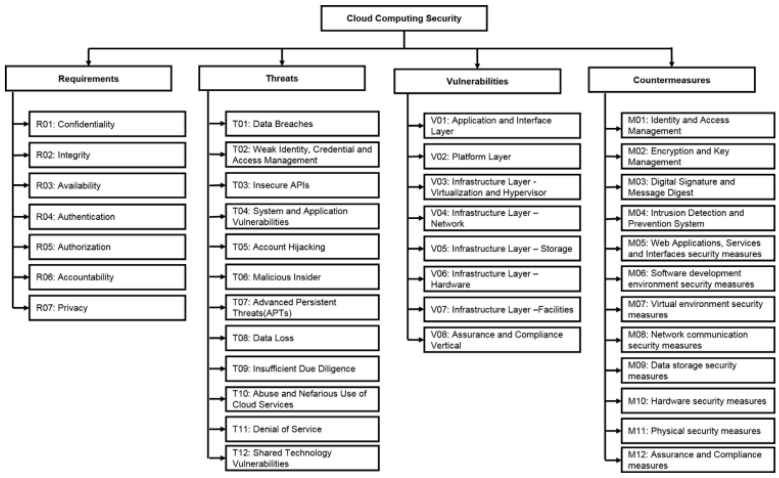


Figura 9: Seguridad en la cloud computing

Fuente: *[138]*

1.8.4.4 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.

1.8.4.4.1 Carencia 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 desde las aplicaciones cliente hasta los servidores, de manera cifrada utilizando algún algoritmo de cifrado como AES, RSA o un híbrido y en el caso de que los servidores estén en la cloud, el autor Yang [139] 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 [140], 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, 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 [141], si un hacker la obtiene podría fácilmente desencriptar toda la información que fluya entre las aplicaciones clientes.

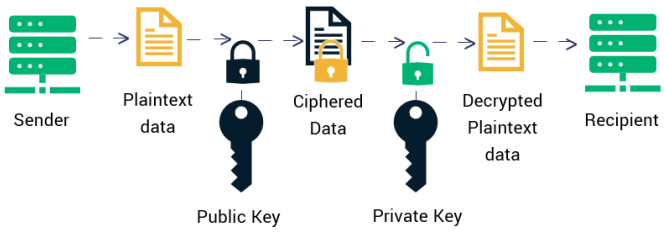


Figura 10: Algoritmo RSA

Fuente: Elaboración propia

1.8.4.4.2 Carencia 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 [142].

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 [143].

1.8.4.4.3 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 [144] y así robar información como claves, cuentas de usuarios, datos de tarjetas de crédito entre otros.

1.8.4.4.4 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 [145], 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.

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

Actualmente, la mayoría de aplicaciones se construye bajo la arquitectura de microservicios, donde la seguridad en las API es un aspecto primordial en dichas arquitecturas para 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 [146].

Entre las maneras propuestas para mitigar las vulnerabilidades en las API están las siguientes [147]:

- 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.

1.8.4.4.6 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 [148]:

- 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.

1.8.4.4.7 Estafas al vender o comprar productos online.

Muchas grandes empresas como Alibaba, Facebook, Instagram, Amazon han optado por la utilización de los marketplaces, que son aplicaciones donde muchas negocios ofertan sus productos y cualquier persona puede crearse una cuenta, provocando un aumento del índice de estafas en compras y ventas 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.

1.8.4.4.8 Metodología Agile Block Chain Dapp Engineering .

La metodología ABCDE se fundamenta en los principios de una metodología ágil debido a que fue creada a partir de la metodología SCRUM por lo tanto utiliza varias prácticas como [149]:

- Enfoques de desarrollo interactivos e incrementales
- Historias de usuarios.
- Roles y reuniones.
- Diagrama derivado del UML para modelar eficazmente la estructura de datos de los smart contracts.
- Diagramas de secuencias para intercambiar mensajes entre las entidades del sistema.
- Utiliza dos flujos para las actividades, el primero tiene que ver con los contratos inteligentes y el segundo con los softwares que interactúan con los DLT.

Un punto a tomar en cuenta es que esta metodología considera dos tipos de integraciones, la del software entre los componentes de los DLT (smart contracts, biblioteca, estructura de datos etc) y los componentes fuera de los DLT como microservicios y aplicaciones web o móvil, naciendo de aquí un completo sistema DApp [150].

La metodología ABCDE utiliza actividades como el diseño, desarrollo, pruebas e integración con Smart contracts y software fuera de los DLT, documentar los Smart contracts utilizando diagramas para su posterior evaluación de seguridad y mantenimiento [151]. En la figura 12, se

presenta de manera gráfica como es el flujo de actividades propuestos por la metodología ABCDE.

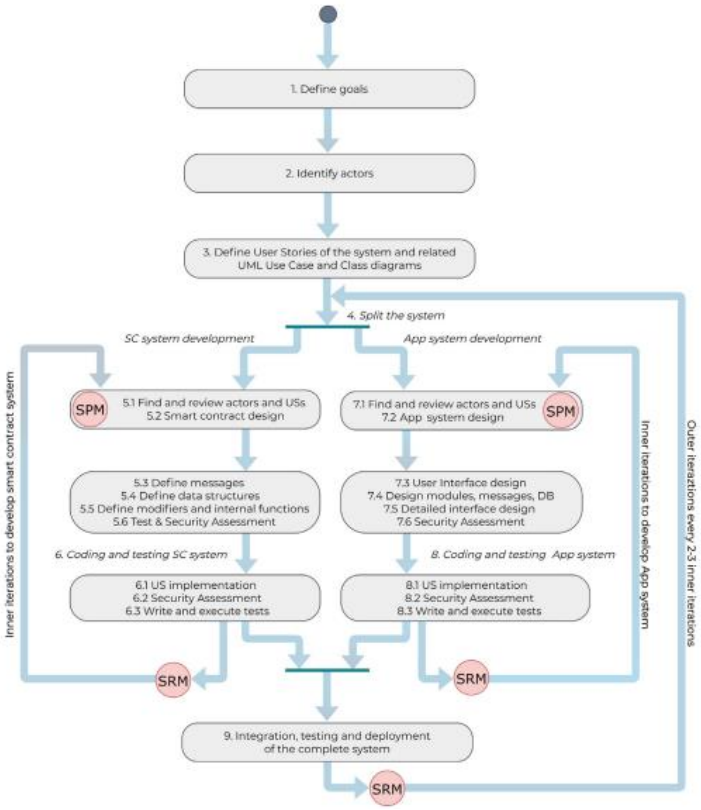


Figura 11: Proceso de la metodología ABCDE

Fuente: *[149]*

Con lo anteriormente mencionado por los autores acerca de la metodología ABCDE, se utilizará la misma en esta investigación porque quedó demostrado que son adecuadas para ser implementadas en aplicaciones basadas en DLT donde los requerimientos varían constantemente por la volatibilidad de los DLT y también porque ofrece una metodología para la correcta utilización de los contratos inteligentes en Dapps.

1.9 Antecedentes contextuales.

1.9.1 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” [152]. 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 [153], 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.

1.9.2 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.

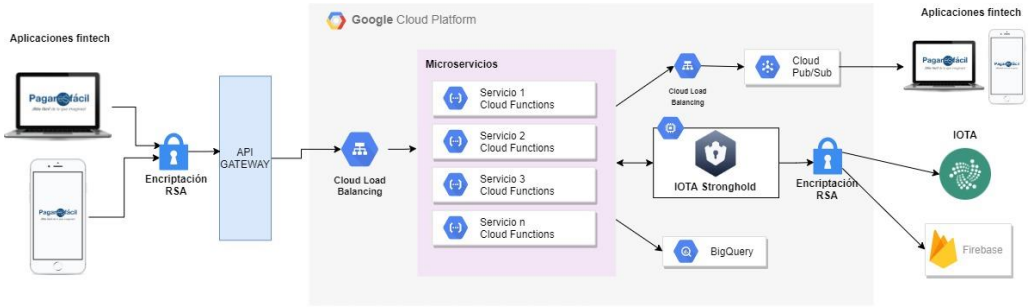


Figura 13: Arquitectura en transacciones financieras con IOTA

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.

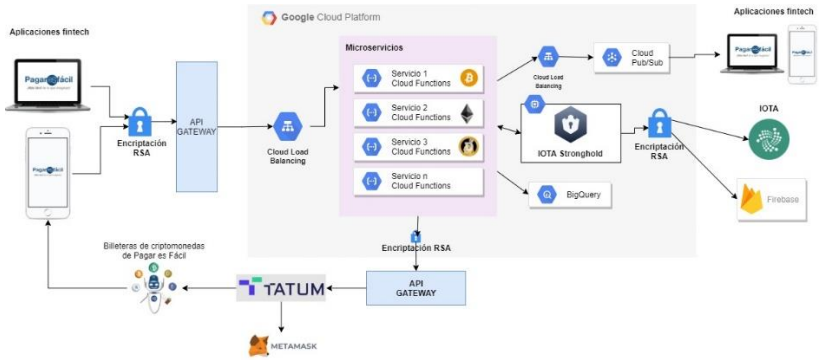


Figura 14: Arquitectura para transferencias internas y externas de criptomonedas

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.

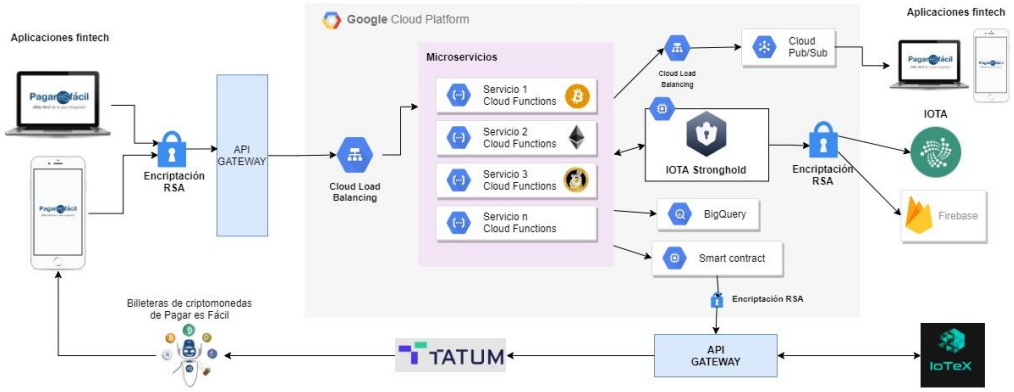


Figura 15: Arquitectura para marketplace usando smart contracts de Iotex

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	Pagos con QR Code	Almacenamiento de transacciones con Iota
16	Verificación de identidad	MATI y almacenamiento en Iota
17	Verificación de registro de tarjetas de crédito	Almacenamiento de transacciones con Iota
18	Compra de acciones	Almacenamiento de transacciones con Iota

Tabla 4: Funcionalidades transaccionales de Pagar es Fácil

Fuente: Datos estadísticos obtenidos de la plataforma

Bibliografía

[1] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey y S. Linkman, «Systematic literature reviews in software engineering – A systematic literature review,» *Information and Software Technology*, vol. 51, nº 1, pp. 7-15, 2009.

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

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

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

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

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

[15] 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.

[16] 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,.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

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

[26] 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.

[27] 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.

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

[29] 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.

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

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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].

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

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

[47] 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.

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

[49] 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.

[50] A. Hannousse y S. Yahiouche, «Securing microservices and microservice architectures: A systematic mapping study,» *Computer Science Review,* vol. 41, 2021.

[51] N. Mateus-Coelho, M. Cruz-Cunha y L. G. Ferreira, «Security in Microservices Architectures,» *Procedia Computer Science,* vol. 181, pp. 1225-1236, 2021.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] 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.

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

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

[59] 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.

[60] 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.

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

[62] 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.

[63] 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.

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

[65] 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.

[66] 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.

[67] 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.

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] 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.

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

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

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

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

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

[78] 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.

[79] 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.

[80] 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.

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

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

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

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

[85] 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.

[86] 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].

[87] I. Team, «Introducing IOTA Stronghold,» 19 07 2020. [En línea]. Available: https://blog.iota.org/iota-stronghold-6ce55d311d7c/. [Último acceso: 20 01 2022].

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

[89] E. A. Kirillova, U. M. Yakhutlov, X. Wenqi, G. Huiting y W. Suyu, «Information 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[109] L. Marchesi, M. Marchesi y R. Tonelli, «ABCDE - agile Block Chain DApp Engineering,» *Blockchain: Research and Applications,* vol. 1, nº 1, 2020.

[110] A. Pinna, G. Baralla, M. Marchesi y R. Tonelli, «Raising Sustainability Awareness in Agile Blockchain-Oriented Software Engineering,» *IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER),* pp. 696-700, 2021.

[111] M. Marchesi, L. Marchesi y R. Tonelli, «An Agile Software Engineering Method to Design Blockchain Applications,» *Association for Computing Machinery*, 2018.

[12] 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].

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