**Evidencia:** Informe de antecedentes conceptuales

**Fecha:** 24-10-2021

* 1. Antecedentes conceptuales.
     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:** Si se utiliza las tecnologías de registros distribuidos (DLT) en arquitecturas informáticas entonces incrementaría la probabilidad de ganar disputas financieras en casos de estafas y fraudes de primera persona en transacciones financieras online de una aplicación Fintech.

**Ho:** Si se utiliza las tecnologías de registros distribuidos (DLT) en arquitecturas informáticas entonces no incrementaría la probabilidad de ganar disputas financieras en casos de estafas y fraudes de primera persona en transacciones financieras online de una aplicación Fintech.

* + 1. Red de categorías de las variables.
       1. Variable independiente.
* Tecnologías de registros distribuidos (DLT) en microservicios cloud.
  + - 1. Variable dependiente.
* Disputas financieras por 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. 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. 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. 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 en un ambiente de sistemas DApps en el contexto de aplicaciones Fintech en un ledger centralizado en comparación con un ledger descentralizado.

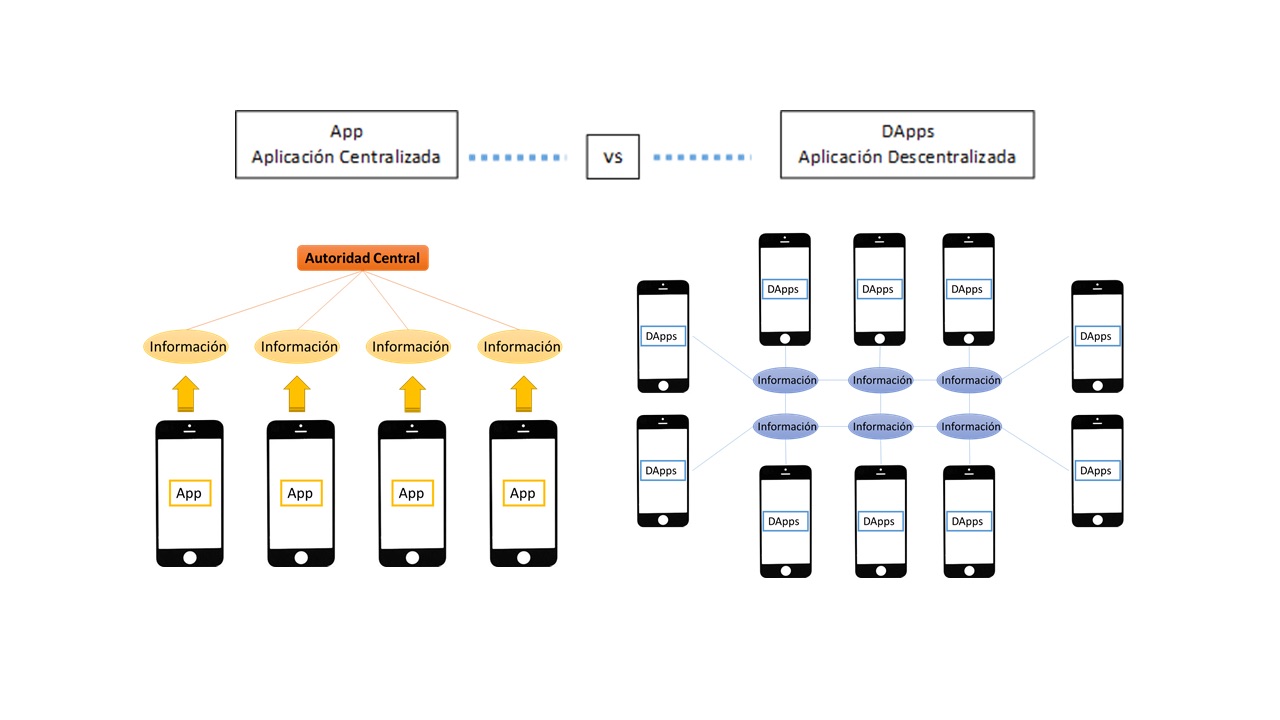


Figura 3: Ledger centralizado y descentralizado en un ambiente Fintech

**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).



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. 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].

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.

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.

Plataformas blockchain

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

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

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.



Figura 6: Ejemplo de un smart contract con iotex

***Fuente:*** *Elaboración propia.*

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].

Estándar ERC-721.

El estándar ERC-721 es un tipo especial de smart contract creado bajo la infraestructura de Ethereum con el objetivo de crear tokens únicos, no fungibles y no intercambiables. Gracias a este estándar se han creado los NFT’s y la identidad digital en aplicaciones informáticas [114].

Estándar ERC-20.

El estándar ERC-20 goza de una estructura pre-programada diseñada para facilitar la implementación de smart contract bajo cualquier blockchain de tipo Ethereum, por tal motivo es el más popular para implementar nuevos smart contracts [115].

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 [116].

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” [117]. Tatum admite las siguientes redes de blockchain para su desarrollo e implementación [118]:

* 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.
  + - * 1. 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) [119] 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 [120], en la figura 7 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 [121].

Entre las ventajas que ofrece Tangle, los autores [119], [120] & [121] 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.

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” [122].

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 [123]. Su principal objetivo es la seguridad durante el flujo de la información en especial para el ambiente Iot [124].

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 [125] [126] pero esto se quiere solucionar con el nuevo protocolo conocido como chrysalis con la salida de IOTA 2.0 nectar reléase [127].

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.

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 [128]. Gracias a esta librería, aumentaría la seguridad al momento de trabajar con contraseñas, llaves privadas o información sensible generadas en transacciones financieras Fintech.

* + 1. Fundamentación teórica de la variable dependiente.
       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 [129].

El objetivo principal de los S.I, según los autores Kirillova & otros [130] 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 [131].

La detección de riesgos por lo general se los realiza en un ambiente de pruebas, el autor Wang [132] 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 8 se muestran más aspectos del mismo.



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

**Fuente:** [132]

* + - 1. 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 [133].

Sin embargo, el autor Tirumala [134] 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 [135] y a la creatividad de los atacantes en utilizar la ingeniería social para penetrar sistemas [136].

* + - 1. 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 [137]. 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 [138], 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 [139] elaboró un organigrama jerárquico (ver figura 9) 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:** [139]

* + - 1. 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. 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 [140] 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 “Pay2Meta” 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 [141], en la figura 10 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 [142], 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. 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 [143].

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 [144].

* + - * 1. 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 [145] y así robar información como claves, cuentas de usuarios, datos de tarjetas de crédito entre otros.

* + - * 1. 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 [146], 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. 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 [147].

* + - * 1. 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. 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. 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. 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 11, 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.

# Bibliografía

|  |  |
| --- | --- |
| [1] | 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. |
| [2] | A. Hannousse y S. Yahiouche, «Securing microservices and microservice architectures: A systematic mapping study,» *Computer Science Review,* vol. 41, 2021. |
| [3] | N. Mateus-Coelho, M. Cruz-Cunha y L. G. Ferreira, «Security in Microservices Architectures,» *Procedia Computer Science,* vol. 181, pp. 1225-1236, 2021. |
| [4] | 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. |
| [5] | 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. |
| [6] | 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. |
| [7] | 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. |
| [8] | 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. |
| [9] | G. S. Sadasiuvam, «A critical review on using blockchain technology in education domain,» *Handbook of Deep Learning in Biomedical Engineering,* pp. 85-121, 2021. |
| [10] | N. O. Nawari y Shriraam Ravindran, «Blockchain and the built environment: Potentials and limitations,» *Journal of Building Engineering,* vol. 25, 2019. |
| [11] | 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. |
| [12] | 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. |
| [13] | X. Fu, H. Wang y P. Shi, «A survey of Blockchain consensus algorithms: mechanism, design and applications,» *Science China Information Sciences,* vol. 64, 2021. |
| [14] | 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. |
| [15] | 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. |
| [16] | Y. Lu, «The blockchain: State-of-the-art and research challenges,» *Journal of Industrial Information Integration,* pp. 80-90, 2019. |
| [17] | 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. |
| [18] | 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. |
| [19] | 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. |
| [20] | 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. |
| [21] | 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. |
| [22] | 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. |
| [23] | 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. |
| [24] | 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. |
| [25] | C. Laneve y C. S. Coen, «Analysis of smart contracts balances,» *Blockchain: Research and Applications,* 2021. |
| [26] | Q. Wang, R. Li, Q. Wang y S. Chen, «Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges,» *Cryptography and Security,* 2021. |
| [27] | T. Hewa, M. Ylianttila y M. Liyanage, «Survey on blockchain based smart contracts: Applications, opportunities and challenges,» *Journal of Network and Computer Applications,* vol. 177, 2021. |
| [28] | N. Khan, B. Kchouri, N. A. Yatoo, Z. Kräussl, A. Patel y R. State, «Tokenization of sukuk: Ethereum case study,» *Global Finance Journal,* 2020. |
| [29] | Tatum, «Welcome to Tatum,» 2021. [En línea]. Available: https://docs.tatum.io/. [Último acceso: 02 11 2021]. |
| [30] | Tatum, «Supported Blockchains,» 2021. [En línea]. Available: https://docs.tatum.io/supported-blockchains. [Último acceso: 02 11 2021]. |
| [31] | 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. |
| [32] | 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. |
| [33] | 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. |
| [34] | S. Popov y W. Buchanan, «FPC-BI: Fast Probabilistic Consensus within Byzantine Infrastructures,» *arXiv,* 2021. |
| [35] | S. Popov, «IOTA: Feeless and Free,» *IEEE Blockchain Technical Briefs,* 2019. |
| [36] | A. Panarello, N. Tapas, G. Merlino, F. Longo y A. Puliafito, «Blockchain and IoT Integration: A Systematic Survey,» *Sensors,* vol. 18, nº 8, 2018. |
| [37] | I. Foundation, «The Coordicide,» 2019. [En línea]. Available: https://files.iota.org/papers/20200120\_Coordicide\_WP.pdf. |
| [38] | 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. |
| [39] | 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]. |
| [40] | 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]. |
| [41] | I. Team, «Introducing IOTA Stronghold,» 19 07 2020. [En línea]. Available: https://blog.iota.org/iota-stronghold-6ce55d311d7c/. [Último acceso: 20 01 2022]. |
| [42] | 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. |
| [43] | 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. |
| [44] | 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. |
| [45] | 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. |
| [46] | 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. |
| [47] | 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. |
| [48] | 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. |
| [49] | Z. Wang, L. Sun y H. Zhu, «Defining Social Engineering in Cybersecurity,» *IEEE Access,* vol. 20, pp. 85094-85115, 2020. |
| [50] | 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. |
| [51] | 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. |
| [52] | R. Kumar y R. Goyal, «On cloud security requirements, threats, vulnerabilities and countermeasures: A survey,» *Computer Science Review,* vol. 33, pp. 1-48, 2019. |
| [53] | 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. |
| [54] | 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. |
| [55] | P. Kumar y S. B. Rana, «Development of modified AES algorithm for data security,» *Optik,,* vol. 127, nº 4, pp. 2341-2345, 2016. |
| [56] | 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. |
| [57] | E. Huseynov y J.-M. Seigneur, «Chapter 50 - Context-Aware Multifactor Authentication Survey,» *Computer and Information Security Handbook (Third Edition),* pp. 715-726, 2017. |
| [58] | 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. |
| [59] | 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. |
| [60] | B. L. y G. M., Microservices: The Evolution and Extinction of Web Services?, Springer, Cham, 2020. |
| [61] | 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. |
| [62] | L. Marchesi, M. Marchesi y R. Tonelli, «ABCDE - agile Block Chain DApp Engineering,» *Blockchain: Research and Applications,* vol. 1, nº 1, 2020. |
| [63] | 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. |
| [64] | M. Marchesi, L. Marchesi y R. Tonelli, «An Agile Software Engineering Method to Design Blockchain Applications,» *Association for Computing Machinery,* 2018. |