

**UNIVERSIDAD TÉCNICA DE MACHALA**

Maestría en Software

**Asignatura:**  
Titulación II  
  
  
**Tema:**

**Taller N° 1: Primeros pasos del Método Científico**

**Docente:**

Walter Fuertes Díaz, PhD

**Estudiante:**

Ing. Jimmy Fernando Castillo Crespín

2021-2022

**Tema de investigación:** Implementación de DLTs para el almacenamiento seguro de transacciones financieras en aplicaciones Fintech.

**Formular un problema de investigación.**

Los datos generados por las aplicaciones Fintech durante las transacciones financieras son de alto valor y contienen información sensible en muchos aspectos y es de conocimiento público por noticias o artículos de los últimos años, los constantes robos de información, fraudes y estafas cometidas por estas aplicaciones que no implementan un sistema de seguridad robusto. Por tal motivo, acceder a estos datos tanto personales como financieras es un objetivo primordial para los hackers de todo el mundo.

Debido a la aparición del COVID-19, se han detectado un aumento progresivo de robos de información, fraudes y estafas en transacciones financieras online ocurridas especialmente entre los años 2020-2021. Estos problemas ocasionarían que las personas dejen de confiar en realizar transacciones financieras online en aplicaciones Fintech.

Por tal razón, la comunidad científica ofrece soluciones aplicada a la seguridad en las transacciones financieras online como encriptaciones avanzadas y aprobadas mundialmente como AES o RSA para la protección de la información desde el lado del cliente o la aplicación de varias metodologías de modelado de amenazas como STRIDE, TRIKE, VAST y PASTA para mitigar ataques en diferentes aplicaciones Fintech, sin embargo, esto no basta para mitigar por completo todas las amenazas.

|  |  |  |
| --- | --- | --- |
| **Causas (Independiente)** | **Problema** | **Consecuencias (dependiente)** |
| * Deficiencia de encriptaciones. * Carencia de implementación de estándares de seguridad. * Carencia de implementación de arquitecturas cloud. * Registro de usuarios sin la suficiente verificación. * Carencia de implementaciones con base de datos descentralizadas (DLT). | **Vulnerabilidades en transacciones financieras en aplicaciones fintech**  **¿En dónde?**  Plataforma Fintech “Pagar es Fácil”  **¿Quiénes son los afectados?**  Usuarios de la plataforma y Stakeholders del proyecto | * Pérdidas económicas. * Pérdida de reputación las aplicaciones Fintech. * Suplantación de identidad. * Robo de información sensible. * Estafas. * Fraudes. |

**Variables independientes:** Arquitectura cloud y tecnologías de registros distribuidos.

**Variables dependientes:** estafas, fraudes y suplantación de identidad.

**Pregunta de investigación.**

¿Cómo la implementación de las tecnologías de registros distribuidos (DLT) en ambientes cloud influyen en la seguridad con respecto a fraudes, estafas y suplantación de identidad en las transacciones financieras realizadas en la plataforma fintech “Pagar es Fácil” durante el primer semestre del 2022?

**Objetivo de la investigación.**

Implementar tecnologías de registros distribuidos bajo la arquitectura de Google Cloud utilizando IOTA, IOTEX y Tatum para mitigar casos de fraudes, estafas y suplantación de identidad en las transacciones financieras realizadas por los usuarios de la plataforma Fintech “Pagar es Fácil”.

**Preguntas secundarias de la investigación**

|  |  |
| --- | --- |
| **Preguntas secundarias** | **Objetivos específicos.** |
| ¿Cuáles son los estudios existentes sobre DLT y algoritmos de encriptaciones para la mitigación de vulnerabilidades en aplicaciones Fintech? | Investigar técnicas DLT y algoritmos de encriptaciones para mitigar vulnerabilidades en aplicaciones Fintech mediante un SLR. |
| ¿Cómo se implementa el estándar de seguridad X.805 en una arquitectura de software cloud para garantizar la seguridad de extremo a extremo en aplicaciones de software? | Diseñar e implementar una arquitectura de software en Google Cloud basado en el estándar de seguridad X.805 para garantizar la seguridad de extremo a extremo en aplicaciones de software. |
| ¿Cómo se implementa registros transaccionales de coste cero para mitigar casos de fraudes en transacciones financieras? | Implementar registros transaccionales de coste cero con IOTA para mitigar casos de fraudes en transacciones financieras. |
| ¿Cómo se implementa una identidad digital descentralizada con blockchain para mitigar la suplantación de identidad de usuarios no verificados? | Programar e implementar NFT’s con Tatum para mitigar la suplantación de identidad de usuarios no verificados. |
| ¿Cómo se implementa los smarts contracts para mitigar casos de estafas en transacciones financieras? | Programar e implementar smarts contracts con IOTEX para mitigar casos de estafas en transacciones financieras. |
| ¿Cómo se implementa algoritmos de encriptaciones y microservicios con DLT en aplicaciones web y móvil para mitigar el robo de información sensible? | Diseñar e implementar aplicaciones Fintech web y móvil con diferentes microservicios DLT y algoritmos de encriptaciones para mitigar el robo de información sensible de usuarios. |

**Análisis de literatura.**

Existe una constante que no puede dejarse de lado en cualquiera de las formas de pagos online existentes actualmente y es que se han detectado un aumento progresivo de fraudes, estafas y robo de información tanto personal como de las tarjetas [1], estos problemas ocasionarían que las personas dejen de confiar en realizar compras online afectando así a millones de aplicaciones Fintech. Por tal razón, la comunidad científica ofrece soluciones aplicada a la seguridad en las transacciones financieras online como encriptaciones avanzadas y aprobadas mundialmente como AES o RSA para la protección de la información desde el lado del cliente, base de datos criptográficas en la nube como IOTA stronghold utilizada para la protección de secretos digitales (tokens, passwords etc) [2] y el uso de los DLT (tecnología de contabilidad distribuida) como una nueva forma de protección de datos dado a las ventajas que ofrece como almacenamiento distribuido, uso de métodos criptográficos que garantizan seguridad, inmutabilidad y encriptación de la información [3]. Brindar seguridad en los pagos online es de especial importancia debido a que potenciaría la confianza de los usuarios en el uso de aplicaciones Fintech.

La propuesta de esta investigación surge tras las alertas de robos, fraudes y estafas en transacciones financieras online ocurridas especialmente entre los años 2020-2021 debido a la aparición del COVID-19 [4], esta pandemia mundial ha sido positiva en cierta medida para la industria de pagos digitales, según cifras de Mastercad y Americas Market Intelligence [5], se duplicó el número de personas que se volcaron a las transacciones online pasando del 45% al 83%, la explicación para este comportamiento es sencillo, las cuarentenas impuestas por los gobiernos mundiales obligaron a las personas a realizar pagos online, potenciando indirectamente el crecimiento exponencial de las aplicaciones Fintech [6]. El COVID-19 también afectó significativamente el mercado de las criptomonedas [7] detectándose un incremento de usuarios y de mercados Fintech que se volcaron al trading de estas [8] y a su vez el interés de los hackers por encontrar vulnerabilidades en estas [9].

Los datos generados por las aplicaciones Fintech durante las transacciones financieras son de alto valor y contienen información sensible en muchos aspectos y es de conocimiento público por noticias o artículos de los últimos años, los constantes robos de información, fraudes y estafas cometidas por estas aplicaciones que no implementan un sistema de seguridad robusto. Por tal motivo, acceder a estos datos tanto personales como financieras es un objetivo primordial para los hackers de todo el mundo. Estas vulnerabilidades se encuentran bien detalladas en el trabajo realizado por los autores Kaur, LashKari & Habibi [10], donde concluyeron que hasta en la actualidad aún siguen existiendo vulnerabilidades humanas, tecnológicas y de transacciones presentes en aplicaciones financieras. Los mismos autores Kaur, LashKari & Habibi [11] en otro de sus artículos dieron más ejemplos de amenazas cibernéticas y las motivaciones que impulsan estos incidentes, aplicaron varias metodologías de modelado de amenazas como STRIDE, TRIKE, VAST y PASTA para mitigar ataques en diferentes aplicaciones Fintech, sin embargo, esto no bastó para mitigar por completo todas las amenazas. Finalmente, el trabajo de los autores Huh, Cho & Kim [12] donde se implementó un sistema de encriptación de datos utilizando RSA para la protección de llaves privadas generados por Ethereum, una de las plataformas blockchain más populares actualmente, incluso en este trabajo no se han tomado en consideración otras medidas de seguridad presentes en los trabajos de Kaur, LashKari & Habibi. Se evidencia que, en los trabajos anteriormente citados, muchas plataformas Fintech no cuentan con la seguridad suficiente para realizar transacciones financieras, inclusive cuando estas transaccionan con criptomonedas [13], surgiendo soluciones como los contratos inteligentes o smart contracts para la mitigación de fraudes y estafas financieras, siendo la red Ethereum la más utilizada para esta labor [14] [15]. Este asunto tan importante ha sido ignorado por la mayoría de empresas desarrolladoras de software por el afán de lanzar aplicaciones Fintech y ganar mercado en estos tiempos de pandemia [16].

**Plantear una posible solución (prognosis) en función de análisis del E.A.**

* Arquitectura de software:
  + Aplicar el estándar X.805 para brindar seguridad a las diferentes capas de la arquitectura de software diseñada e implementada en Google Cloud.
  + Implementar los diferentes DLT mediante el uso de IOTA, IOTEX y Tatum para brindar seguridad a todos los microservicios alojados en Google Cloud.
* Software
  + Desarrollar las aplicaciones web y móvil necesarias donde se testearán el funcionamiento de los DLT en diferentes transacciones financieras.

**Plantear la idea de investigación (prognosis).**

* Evaluación y selección de tecnologías de registros distribuidos.
* Diseño de las arquitecturas de software.
* Implementación de las arquitecturas de software.
* Implementación de los microservicios con DLT en funcionalidades transaccionales.
* Desarrollo e implementación de las aplicaciones clientes.
* Desarrollar las pruebas funcionales.
* Evaluación y validación de resultados.

**Plantear una primera hipótesis.**

**Hi:** La implementación de tecnologías de registros distribuidos (DLT) en arquitecturas cloud incrementa la seguridad durante el almacenamiento de transacciones financieras en aplicaciones Fintech logrando mitigar casos de fraudes, estafas y suplantación de identidad.

**Ho:** La implementación de tecnologías de registros distribuidos (DLT) en arquitecturas cloud no incrementa la seguridad durante el almacenamiento de transacciones financieras en aplicaciones Fintech para mitigar casos de fraudes, estafas y suplantación de identidad.

**Plantear los productos entregables.**

* Aplicaciones Fintech web y móvil.
* Códigos de programación con la aplicabilidad de los DLT.
* Diagramas de arquitecturas de software en Google cloud.

# Bibliografía

|  |  |
| --- | --- |
| [1] | A. Pawlicka, M. Choraś, M. Pawlicki y R. Kozik, «A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic,» *Business Horizons,* 2021. |
| [2] | IOTA, «IOTA Stronghold,» 2021. [En línea]. Available: https://stronghold.docs.iota.org/docs/welcome. [Último acceso: 2021]. |
| [3] | A. Panwar y V. Bhatnagar, «Distributed Ledger Technology (DLT): The Beginning of a Technological Revolution for Blockchain,» *2nd International Conference on Data, Engineering and Applications (IDEA),* pp. 1-5, 2020. |
| [4] | J. D. N. I. M. A. H. Y. B. d. l. Á. &. V. M. J. A. Tello Saldaña, «Impacto de los canales de comercialización online en tiempos del COVID-19,» *INNOVA Research Journal,* vol. 5, nº 3, pp. 15-39, 2020. |
| [5] | A. M. Intelligence, «La aceleración de la inclusión financiera durante la pandemia de COVID-19. Oportunidades ocultas que salen a relucir,» 2020. [En línea]. Available: https://www.mastercard.com/news/media/qdxlk0nc/ami\_201016\_mastercard\_financial\_inclusion\_during\_covid\_es\_short\_03-1.pdf. [Último acceso: 2021]. |
| [6] | M. T. Le, «Examining factors that boost intention and loyalty to use Fintech post-COVID-19 lockdown as a new normal behavior,» *Heliyon,* vol. 7, nº 8, 2021. |
| [7] | S. Lahmiri y S. Bekiros, «The effect of COVID-19 on long memory in returns and volatility of cryptocurrency and stock markets,» *Chaos, Solitons & Fractals,* vol. 151, 2021,. |
| [8] | 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. |
| [9] | C. F. Security, «Cybercrime in a time of coronavirus,» *Computer Fraud & Security,* vol. 2020, nº 5, pp. 1-3, 2020. |
| [10] | 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. |
| [11] | 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. |
| [12] | S. Huh, S. Cho y S. Kim, «Managing IoT devices using blockchain platform,» *19th International Conference on Advanced Communication Technology (ICACT),* pp. 464-467, 2017. |
| [13] | D. Luo, T. Mishra, L. Yarovaya y Z. Zhang, «Investing during a Fintech Revolution: Ambiguity and return risk in cryptocurrencies,» *Journal of International Financial Markets, Institutions and Money,* vol. 73, 2021. |
| [14] | G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali y R. Hierons, «Smart contracts vulnerabilities: a call for blockchain software engineering?,» *International Workshop on Blockchain Oriented Software Engineering (IWBOSE),* pp. 19-25, 2018. |
| [15] | L. Liu, W.-T. Tsai, M. Z. A. Bhuiyan, H. Peng y M. Liu, «Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum,,» *Future Generation Computer Systems,* 2021. |
| [16] | P. K. Ozili, «Financial Inclusion and Fintech during COVID-19 Crisis: Policy Solutions,» *The Company Lawyer Journal,* vol. 8, pp. 1-9. |