UNIVERSIDAD TÉCNICA DE MACHALA

Maestría en Software

Asignatura:

Titulación II

Tema:

Taller N° 4: Estructura del Trabajo de Titulación: La Introducción

Docente:

Walter Fuertes Díaz, PhD

Estudiante:

Ing. Jimmy Fernando Castillo Crespín

2021-2022

INTRODUCCIÓN

Desde su creación hace más de 30 años, el internet ha revolucionado el mundo tal y como lo conocemos y actualmente influye en muchos ámbitos sociales, en especial en el campo del comercio electrónico donde se realizan transacciones financieras de manera online desde la comodidad del hogar. Cabe recalcar que los métodos de pagos online mayormente utilizados por las personas en la actualidad son: tarjetas proporcionadas por bancos, transferencias bancarias, pasarelas de pagos entre los que se destaca Paypal como la mayormente utilizada por los negocios e-commerce [1] y finalmente las billeteras virtuales de criptomonedas empleadas principalmente para el trading y compra/venta de activos digitales [2].

Existe una constante que no puede dejarse de lado en cualquiera de las formas de pagos online anteriormente mencionadas y es que se han detectado un aumento progresivo de fraudes, estafas y robo de información tanto personal como de las tarjetas [3], estos problemas ocasionarían que las personas dejen de confiar en realizar compras online, afectando así a millones de aplicaciones Fintech.

Por tal razón, la comunidad científica ofrece soluciones aplicada a la seguridad en las transacciones financieras online como encriptaciones avanzadas y aprobadas mundialmente como AES o RSA para la protección de la información desde el lado del cliente, base de datos criptográficas en la nube como IOTA stronghold utilizada para la protección de secretos digitales (tokens, passwords etc) [4] y el uso de los DLT (tecnología de contabilidad distribuida) como una nueva forma de protección de datos dado a las ventajas que ofrece como almacenamiento distribuido, uso de métodos criptográficos que garantizan seguridad, inmutabilidad y encriptación de la información [5]. Brindar seguridad en los pagos online es de especial importancia debido a que potenciaría la confianza de los usuarios en el uso de aplicaciones Fintech.

La propuesta de esta investigación surge tras las alertas de robos, fraudes y estafas en transacciones financieras online ocurridas especialmente entre los años 2020-2021 debido a la aparición del COVID-19 [6], esta pandemia mundial ha sido positiva en cierta medida para la industria de pagos digitales, según cifras de Mastercad y Americas Market Intelligence [7], se duplicó el número de personas que se volcaron a las transacciones online pasando del 45% al 83%, la explicación para este comportamiento es sencillo, las cuarentenas impuestas por los gobiernos mundiales obligaron a las personas a realizar pagos online, potenciando indirectamente el crecimiento exponencial de las aplicaciones Fintech [8].

El COVID-19 también afectó significativamente el mercado de las criptomonedas [9] detectándose un incremento de usuarios y de mercados Fintech que se volcaron al trading de estas [10] y a su vez el interés de los hackers por encontrar vulnerabilidades en estas [11].

Los datos generados por las aplicaciones Fintech durante las transacciones financieras son de alto valor y contienen información sensible en muchos aspectos [12] y es de conocimiento público por numerosos artículos citados anteriormente, los informes de robos de información, fraudes y estafas cometidas por estas aplicaciones que no implementan un sistema de seguridad robusto [13]. Por tal motivo, detectar estas vulnerabilidades en dichas aplicaciones es un objetivo primordial para los hackers de todo el mundo.

Estas vulnerabilidades se encuentran detalladas en el trabajo realizado por los autores Kaur, LashKari & Habibi [14], donde concluyeron que, hasta en la actualidad, siguen aún existiendo vulnerabilidades humanas, tecnológicas y transaccionales presentes en aplicaciones financieras. Los mismos autores Kaur, LashKari & Habibi [15] 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 [16] 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 [17], surgiendo soluciones como los contratos inteligentes o smart contracts para la mitigación de fraudes y estafas financieras, sobresaliendo Ethereum como la más utilizada para esta labor [18] [19]. 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 [20].

En el trabajo realizado por Gatteschi [21] discute las ventajas y desventajas del blockchain y concluye que esta tecnología puede ser aplicada en cualquier sector, brindando grandes ventajas al sector Fintech [22]. Sin embargo, surgen varias limitantes sobre el uso de la tecnología blockchain demostradas por los autores Gatteschi y Mesengiser & Miloslavskaya [23] que podrían ser un problema a futuro para las aplicaciones Fintech y son el rendimiento, rentabilidad y sostenibilidad con el medio ambiente.

Con respecto al rendimiento, mientras más crece la red de blockchain, mayor será el tiempo de procesamiento de la transacción, bitcoin, por ejemplo, tiene la capacidad de procesar transacciones por segundo muy bajas dependiendo del congestionamiento de la red [24] a

comparación de las 65.000 transacciones por segundo reportas por la empresa Visa en el año 2021 [25], esto afectaría negativamente a las aplicaciones Fintech debido a que las mayorías de estas, son aplicaciones móviles y requieren que estas transacciones sean rápidas y sean reflejadas al usuario en el menor tiempo posible sin afectar la usabilidad.

Con respecto a la sostenibilidad ambiental, los autores Vries & Stoll [26] y Vries [27] analizaron los daños ambientales producidos por las criptomonedas mayormente desarrollados bajo la tecnología blockchain, donde concluyeron que estos daños son exponenciales para el medio ambiente. Esta limitante ocasionaría un problema para muchas aplicaciones, incluidas las Fintech, dado a que a futuro muchas personas, empresas o instituciones gubernamentales como el gobierno de China por ejemplo [28], rechacen utilizar, apoyar o colaborar con aplicaciones desarrollados bajo la tecnología blockchain por el daño al medio ambiente que este ocasiona.

Con respecto a la rentabilidad, será menor a medida del crecimiento del blockchain dado a que genera un abismal consumo energético debido al tiempo que a estos le toman para resolver operaciones matemáticas complejas para concatenarse a la red [29] y a su vez generan residuos electrónicos [30]. Estos problemas se estudiaron mejor en la investigación realizado por Vries & Stoll [26] donde cuantificaron que toda la red del bitcoin genera por año una cantidad de 30,7 kilotoneladas de residuos electrónicos, que, según estos mismos autores, esta cantidad es comparable con los desperdicios generados por equipos electrónicos pequeños del país de Holanda.

Entre las soluciones propuestas a estas limitaciones se encuentran diseñar estrategias de sostenibilidad ambiental para el blockchain propuesta por Bai & Sarkis & Cordeiro [31], los mismo autores Vries & Stoll [26] dan una solución de sustituir el sistema de minera (el protocolo Proof-of-work) en su totalidad, dado a que según los estudios de evaluación de este protocolo realizados por los autores Nair & Dorai [32] y Gemeliarana & Sari [33], concluyeron que la seguridad fue alta pero de rendimiento bajo debido al costo eléctrico alto, surgiendo de aquí propuestas como proof-of-contribution [34] o el proof-of-stake [35].

Es indiscutible que la utilización del blockchain proporciona una solución robusta, gratuita y segura, sin embargo, aplicar solamente blockchain no es suficiente, hay que implementarla en conjunto con otros métodos de seguridad [36], esta problemática surge por la variedad de tecnologías de las cuales están desarrolladas las diferentes aplicaciones que requieren protecciones tanto a nivel de servidores como de aplicación. A raíz de esto surgió IOTA como solución a los problemas de rendimiento, rentabilidad y sostenibilidad presentes en blockchain pero esta tecnología igualmente presenta sus limitaciones ocasionadas por ser una tecnología relativamente nueva [37].

Basados en las afirmaciones anteriores, la presente investigación utilizará el DLT de IOTA como solución a las problemáticas expuestas por los autores [21], [23], [29], [30] y [26] gracias a la creación de IOTA que fue la primera criptomoneda que se creó fuera del sistema blockchain [38], en su lugar utiliza Tangle que a diferencia del blockchain, solamente necesita confirmar dos transacciones de diferentes participantes para poder concatenar su transacción dentro del nodo de Tangle [39], resultando ser rentable para ser utilizado en aplicaciones Fintech debido a la rapidez en la confirmación de las transacción.

El Tangle de IOTA hace posible que no exista la necesidad de utilizar la minería como en blockchain y con esto no se afectaría al medio ambiente, en lugar de esto utiliza los propios dispositivos clientes como verificadores de transacciones; una de las ventajas más sobresalientes para ser utilizado en el internet de las cosas (IoT) [40], [41] y en transacciones financieras debido a que no existen comisiones (fee) [42] que se carguen a las transacciones realizadas por los clientes en aplicaciones Fintech por citar un ejemplo.

Lastimosamente, los smart contracts de IOTA actualmente se encuentra en fase beta [43], lo que impide su implementación en un ambiente de producción, alternativas como Iotex blockchain son viable para aplicaciones Fintech debido a sus bajas comisiones de transacción en comparación a otras blockchain como Ethereum o Cardano [44].

En base al trabajo de Taylor & otros [45] donde se realizó una revisión sistemática de literatura de las ventajas de seguridad cibernética ofrecidas por la utilización del blockchain y en base al trabajo realizado por Ali & otros [46] donde demuestran el estado actual de la utilización de los DLT en el sector financiero, se estableció el objetivo de esta investigación que busca la implementación de los DLT en aplicaciones Fintech para el almacenamiento seguro de las transacciones financieras, tomando en cuenta que la tecnología DLT estará presente en el futuro de la ciberseguridad financiera [47].

Por todo lo anteriormente redactado y con la intención de colaborar con el objetivo 3.7 propuesto en el plan nacional de desarrollo ecuatoriano [48] que incentiva a la producción y consumo ambiental de manera responsable con el fin de incrementar la productividad de tecnologías y así combatir con la obsolescencia programada y a su vez otorgar una adecuada utilidad a la información confidencial de los usuarios así como lo estipula el art. 66, #19 de la Constitución del Ecuador [49] y la Ley de Protección de Datos (LOPD) [50] se realizó esta investigación que tiene como objetivo la implementación de tecnologías de registros distribuidos en una arquitectura de microservicios de Google Cloud utilizando las plataformas de IOTA, IOTEX, Tatum para disminuir casos de delitos informáticos (estafas y fraudes) realizadas en transacciones financieras de una aplicación Fintech, partiendo de la hipótesis de que utilizar DLT en una arquitectura de microservicios cloud disminuye casos de estafas y fraudes, otorgando ventajas como seguridad,

inmutabilidad, integridad, no repudio, disponibilidad y confidencialidad de los datos generados en las transacciones financieras de una aplicación Fintech.

Para el cumplimiento del objetivo detallado anteriormente, se diseñó una aplicación web y móvil las cuales se encuentran funcionando en arquitecturas cloud bajo la plataforma de Google, son diferentes instancias las cuales proporcionan una arquitectura basado en eventos y microservicios, estos microservicios proporcionan las Apis necesarias para el procesamiento de datos a través del protocolo https y la interfaz de programación API-REST y a su vez estos se encargarán de realizar el almacenamiento de los datos en los DLT utilizando IOTA que gracias a su coste cero en sus almacenamientos será utilizado cuando se trate de transacciones financieras generales, se programarán smart contracts utilizando IoTex cuando se trate de compras realizadas en el marketplace y trading de criptomonedas y finalmente se utilizará NFT con Tatum como plataforma blockchain para la identidad digital de los usuarios al realizar transacciones con tarjetas de crédito.

La investigación se realizará en un ambiente de producción, tomando como caso práctico todas las transacciones realizadas por los usuarios en la plataforma de Pagar es Fácil. Luego de la aplicación de las pruebas pertinentes realizadas al finalizar la implementación de la propuesta, se concluye que el Tangle de la plataforma de IOTA y de igual forma el blockchain proporcionado por IoTex y la plataforma Tatum mejoraron la seguridad y disminuyeron casos de fraudes y estafas realizadas por los usuarios en sus transacciones financieras dentro de la plataforma Fintech. Sin embargo, también se debe tener a consideración las altas vulnerabilidades que se encuentran presentes cuando se utilizan pasarelas de pagos desarrollados por terceros. Se recomienda que estos procesos de pagos no solamente dependan de las bondades ofrecidas por blockchain o Tangle sino que también estos pagos tengan certificación PCI DSS mínimo de nivel 3, encriptación de datos de extremo a extremo y una certificación de seguridad como es la ISO 21000:2013.

La siguiente investigación está estructurada en cuatro capítulos comenzando con la introducción donde se indica al lector lo que se va a desarrollar. El capítulo uno trata sobre la elaboración del estado de arte la cual está conformada por los antecedentes históricos, conceptuales y contextuales, todos enfocados a los objetos de estudios que son las Fintech y los DLT. El capítulo dos indica los métodos y metodologías que se utilizaron en la investigación como el tipo de estudio, los enfoques, la población y muestra, métodos teóricos, empíricos y técnicas estadísticas utilizadas. El capítulo tres muestra los resultados obtenidos, fundamentados en los aportes prácticos y teóricos obtenidos en el capítulo dos. El capítulo cuatro se discute los resultados obtenidos con énfasis en aspectos como hallazgos obtenidos, su relación con otros trabajos,

conclusiones y sugerencias para trabajos futuros. Finalmente, se elaboraron las conclusiones obtenidas de la investigación realizada y la bibliografía correspondiente.

Bibliografía

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

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

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

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

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

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

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

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

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

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

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

[12] J. Kang, «Mobile payment in Fintech environment: trends, security challenges, and services,» *Human-centric Computing and Information Sciences,* vol. 8, nº 32, 2018.

[13] S. R. Randy, B. Indra y P. Betty, «Challenges and Trends of Financial Technology (Fintech): A Systematic Literature Review,» *Information,* vol. 11, nº 12, 2020.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[40] 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.

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

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

[43] 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].

[44] 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.

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

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

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

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

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

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