1. 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 ampliamente 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 por 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 motivación 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.

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].

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.

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 [24], 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 [25].

Basados en las afirmaciones anteriores, la presente investigación utilizará el DLT de IOTA como solución a las problemáticas expuestas por los autores [21] y [23]. Gracias a la creación de IOTA que fue la primera criptomoneda que se creó fuera del sistema blockchain [26], 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 [27], 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 dispositivos móviles o un arduino [28], [29] para ser verificadores de transacciones; una de las ventajas más sobresalientes para ser utilizado en el internet de las cosas (IoT) [30], [31], [32] y en transacciones financieras debido a que no existen comisiones (fee) [33] que se carguen a las transacciones realizadas por los clientes en aplicaciones Fintech o en protocolos ligeros para dispositivos Iot [34], [35] en monitoreos con WSN [36] por citar algunos ejemplos.

Lastimosamente, los smart contracts de IOTA actualmente se encuentra en fase beta [37], 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 [38]. En base al trabajo de Taylor & otros [39] 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 [40] 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 [41].

Por todo lo anteriormente redactado, este documento 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 incrementar la probabilidad de ganar disputas de pagos por delitos informáticos (estafas y fraudes de primera persona) 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 e implementó una aplicación web y móvil siguiendo la metodología Agile Blockchain DApps Engineering (ABCDE) las cuales se encuentran funcionando en arquitecturas cloud bajo la plataforma de Google, son diferentes instancias las cuales proporcionan una arquitectura basada en procesamientos complejos de eventos (CEP) [42] 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. La investigación se realizó en un ambiente de producción controlado, tomando como caso práctico las transacciones realizadas por los usuarios en la plataforma Fintech Pay2Meta. Las principales contribuciones se detallan a continuación:

* Implementación de IOTA para garantizar la integridad e inmutabilidad en los registros de las transacciones financieras realizadas por los usuarios en las aplicaciones clientes de la plataforma Pay2Meta.
* Implementación de smart contracts utilizando IoTex para mitigar estafas cuando los usuarios realicen compras o ventas en el marketplace de productos y trading de criptomonedas en la plataforma Pay2Meta.
* Implementación de verificación biométrica con MATI y NFT con Tatum como plataforma Blockchain para obtener una identidad digital de los usuarios al realizar transacciones con tarjetas de crédito o débito en la plataforma Pay2Meta.

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 aumentaron la seguridad y disminuyeron casos de fraudes y estafas de primera persona 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.

El siguiente informe está estructurado de la siguiente manera: la primera sección corresponde a la elaboración del estado de arte la cual está conformada por los antecedentes históricos y conceptuales donde se fundamenta las tecnologías utilizadas en la investigación, así como los trabajos relacionados. La segunda sección explica la propuesta de solución, la tercera sección describe el caso de estudio utilizado que fue la fintech Pay2Meta, la cuarta sección corresponde a todos los experimentos realizados, la quinta sección detalla el análisis de resultados y la última sección exponen las conclusiones y recomendaciones.

1. Estado del arte

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 [43], uno de los primeros sistemas e-commerce que implementaron las ventas online [44] surgiendo desde este momento el término Fintech 1.0 [45].

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 [46]. 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 [47], [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 [48], 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 [49].

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 [50]. Pero esta situación se volvió viable en el año 2009 con la aparición del bitcoin por Satoshi Nakamoto [51] 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 [52] 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 [53].

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) [53] [54], 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 [55]). 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 [56] 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 [57] de las cuales se obtuvieron como resultado su propia blockchain privada denominada Quorum desarrollado bajo el código Ethereum [58] y en el año 2019 lanzaron su propia criptomoneda llamada JPMCoin [59]. Cabe recalcar que Quorum fue diseñado para satisfacer las necesidades de las instituciones financieras [60].

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 [61]) para desarrollar servicios de pagos internacionales dando como resultado su servicio Fintech denominado Santander One Pay FX [62]; 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 [63].

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 [64]. 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) [65] 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 [66] 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], [64], [67] & [68] 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) [69] , un producto de esta nueva tecnología es la red Cardano (criptomoneda ADA) [70].

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) [71].

Gracias al protocolo de consenso de IOTA, llamado FPC (Fast Probabilistics Consensus) [72], 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 [73], haciéndolo perfecto para ser utilizado en micropagos de IoT [74] 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 [75]. 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 [37], 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 [76].

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 [77], pero a su vez se detectaron un incremento de la ciberdelincuencia en estas aplicaciones [78], [79], [80], [81] & [82].

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 [83] & Mohanta y otros [84].

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 [85] 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.

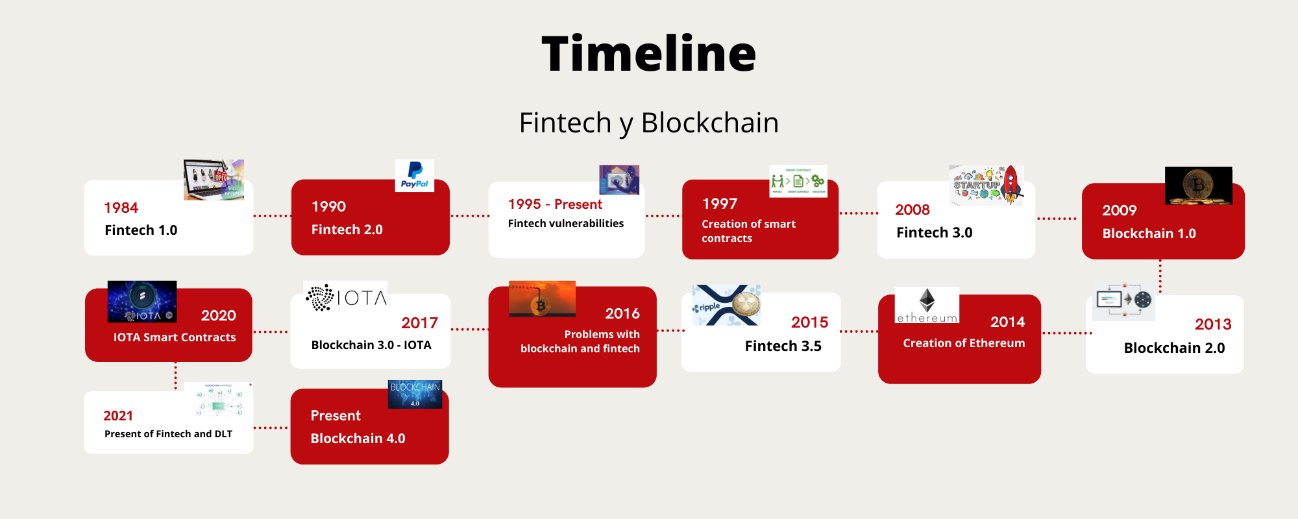


Figure 1: Chronological organization of the history of fintech and blockchain

***Source: self made***

* 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 [86] y distribuidas debido a su potencial de escalabilidad y seguridad para la información [87], esta afirmación viene fundamentada por los autores Hannousse & Yahiouche [88] donde concluyeron que los microservicios nacieron con la finalidad de enfrentar la escalabilidad horizontal y vertical y el mantenimiento 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 [89], 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 [90] y Sheng [91].

* 1. 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 [92], ya que un hacker no podría acceder a esta información debido a que se encontraría distribuida en múltiples servidores. En la figura 2 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.

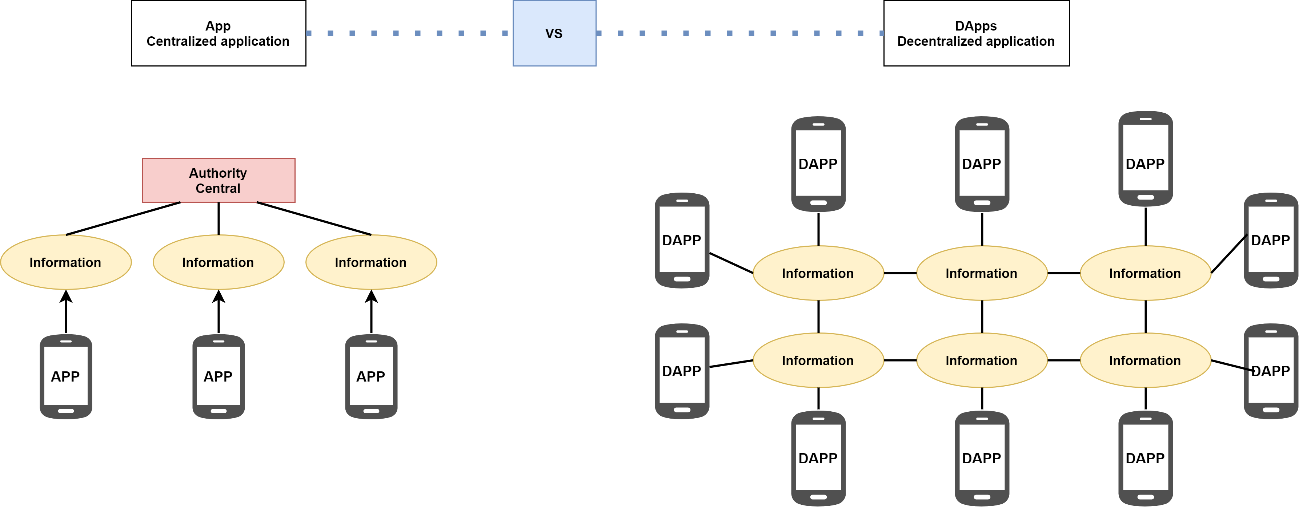


Figure 2: Centralized and decentralized ledger in a Fintech environment

***Source:*** *self made*

Entre las ventajas de los DLT, el autor Hashimy [93] 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 [94] clasifica a los DLT en tres tipos, el blockchain, Tempo Ledger y DAG Ledger, en la figura 3 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 [95] el cual indica que IOTA es un DAG al igual que HyperLedger Fabric que el autor Nawari [96] lo coloca de tipo blockchain y el autor Zhuang lo coloca de tipo DAG.

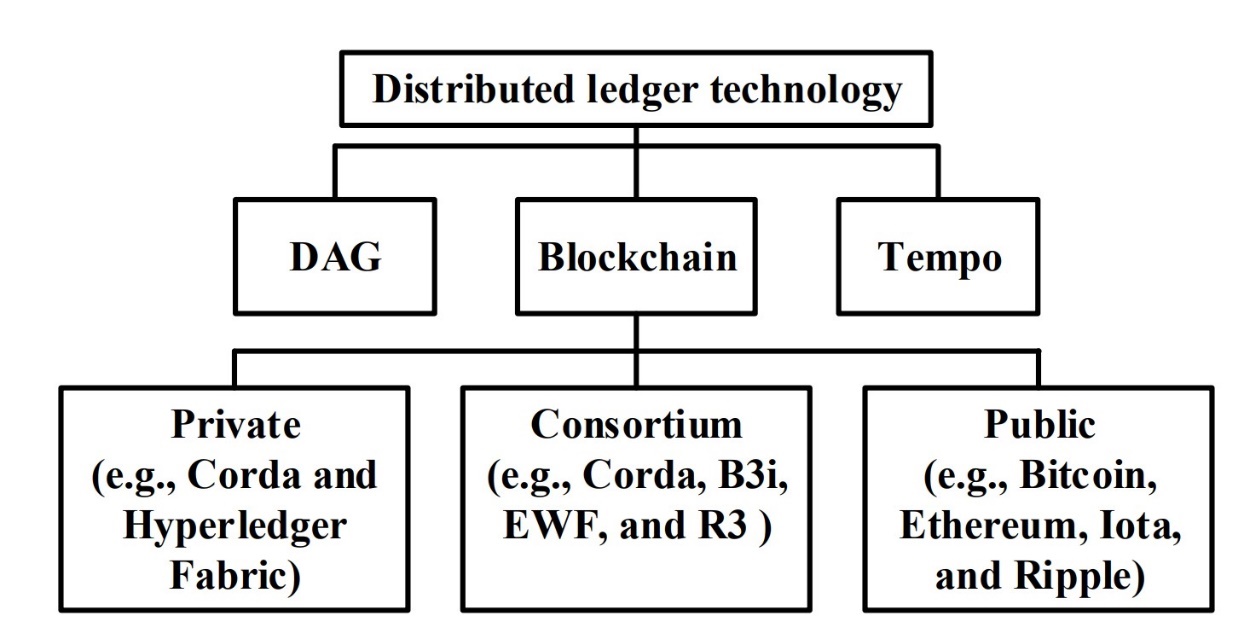


Figure 3: Classification of DLTs

**Source:** Adapted of[94]

En la figura 4, Bahar [97]proporciona más características de los DLT, una de ellas es su amplia aplicación en diferentes campos como puede ser en la medicina, Iot, finanzas, industrias y mucho más, demostrando la gran versatilidad de esta tecnología en ser aplicadas en muchos dispositivos tecnológicos (smart watch, celulares, routers etc).

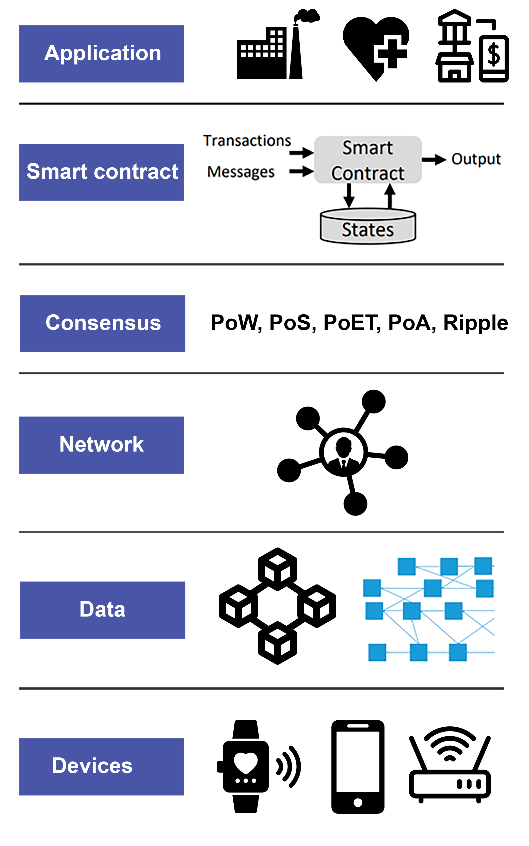


Figure 4: Characteristics of DLTs

**Source:**  Adapted of [97]

Actualmente existen dos estructuras en como la información en los DLT se distribuye dentro de la red, la primera es en forma de cadena de bloques como es el caso del blockchain y como DAG en el caso del Tangle [98] y cada una de ellas manejan sus propios protocolos de consenso entre las más destacadas se encuentran el proof-of-work, proof-of-stake, proof-of-contribution, FPC (IOTA) [99] y también ventajas únicas como la implementación de smart contracts muy baratas con IoTex blockchain [38] o un almacenamiento con coste cero con IOTA [30].

* + 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 [100]. El autor Feng [101] la define como una base de datos distribuida que utiliza el P2P ofreciendo seguridad y privacidad en las transacciones que se registran. Según Karaivanov [102], estas transacciones pueden ser económicas como costosas dependiendo del tipo de información que se desee almacenar.

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 [103].

* + - 1. Tipos de blockchain

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

Permisos de acceso:

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

Privacidad en transacciones:

* Transacciones públicas: cualquier persona puede ver las transacciones.
* Transacciones privadas: solo los usuarios pertenecientes a la red pueden ver las transacciones.
  + - 1. Ventajas del blockchain

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

* Descentralización: las transacciones son procesados por múltiples servidores.
* Trazabilidad: los usuarios pueden estar pendientes del estado de sus transacciones.
* Transparencia: los datos no pueden ser alterados.
* Autonomía: los datos no son regulados por ninguna entidad.
  + - 1. Plataformas blockchain

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

* Bitcoin
* Ethereum
* Hyperledger Fabric
* Tatum
* IBM Blockchain
* Hydrachain
* Ripple
* R3 Corda
* Openchain
  + 1. IOTEX

IoTex es una infraestructura de blockchain cuya principal característica es su protocolo de consenso en tiempo real llamado Roll-DPoS [108] que permite una comunicación rápida y eficaz entre la blockchain y los millones de dispositivos conectados gracias a la web of things (WoT) [109] 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 [110].

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 [38], haciéndola perfecta para ser utilizado para smart contracts por su rapidez y bajo costo en comisiones.

* + 1. 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 [111].

* + 1. 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 [112].

* + 1. 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 [113].

* + 1. 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” [114]. Tatum admite las siguientes redes de blockchain para su desarrollo e implementación [115]:

* 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) [116] 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 [117].

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 [118].

Entre las ventajas que ofrece Tangle, los autores [116], [117] & [118] 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. 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 tecnología robusta, de consenso binario y baja complejidad para comunicarse entre nodos [119].

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 [120]. Su principal objetivo es la seguridad durante el flujo de la información en especial para el ambiente Iot [121].

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 [122] [123] pero esto se quiere solucionar con el nuevo protocolo conocido como chrysalis con la salida de IOTA 2.0 nectar reléase [124].

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 [37] dando un gran paso sobre esta arquitectura.

* + - 1. 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 [125]. Gracias a esta librería, aumentaría la seguridad al momento de trabajar con contraseñas, llaves privadas o información sensible generadas en transacciones financieras Fintech.

* 1. Seguridad informática

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 [126]. El objetivo principal de los S.I, según los autores Kirillova & otros [127] 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 [128].

La detección de riesgos por lo general se los realiza en un ambiente de pruebas, el autor Wang [129] 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 5 se muestran más aspectos del mismo.

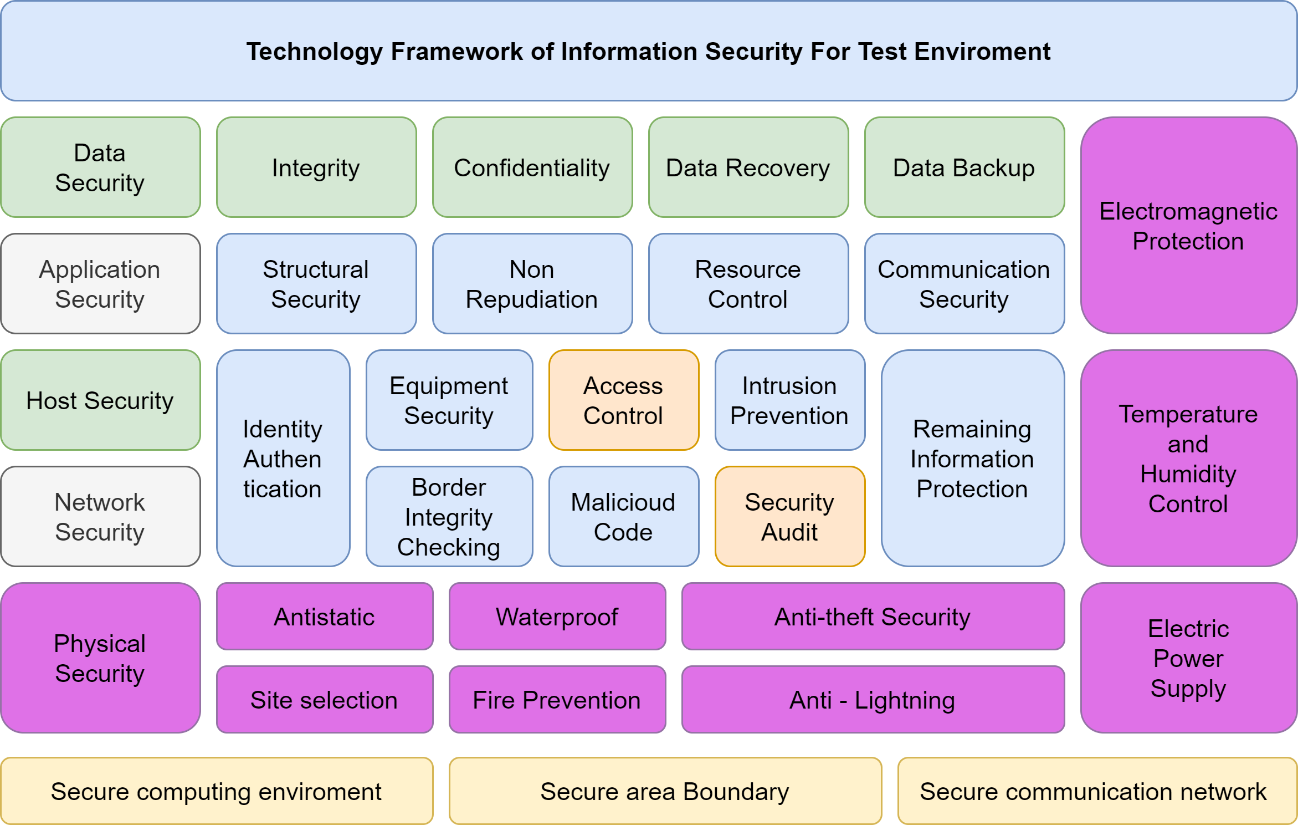


Figure 5: Framework od information security

**Source:**  Adapted of [129]

Del marco de trabajo mencionado anteriormente, esta investigación se enfocó en dar solución a los problemas de la seguridad de datos, integridad, no repudio, confidencialidad, identidad, seguridad en la comunicación entre Apis y seguridad estructural en una aplicación Fintech utilizando smart contract con IOTEX, encriptación RSA e IOTA.

* + 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 [130].

Sin embargo, el autor Tirumala [131] 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 [132] en especial en el ámbito Iot donde amenazas de tipo DDos, man in the middle [133], filtración de datos, falsificación de dispositivos entre otras aún siguen presentes en la actualidad [134].

Con respecto a los ataques man in the middle, en esta investigación se aplicó la encriptación RSA como medida de mitigación a esta vulnerabilidad.

* + 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 [135]. 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 [136], 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 [137] elaboró un organigrama jerárquico (ver figura 6) 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.

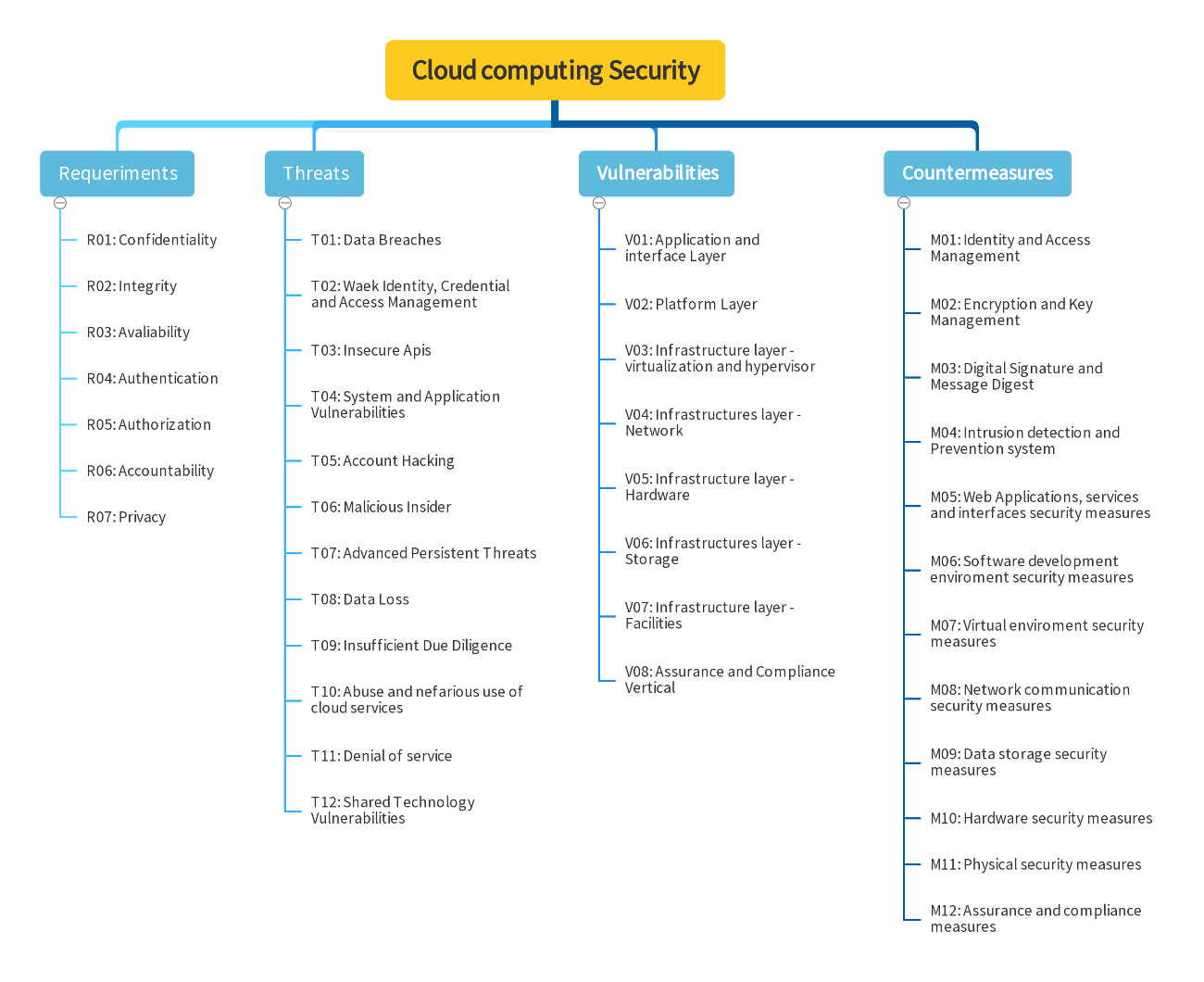


Figure 6: Cloud Computing Security

**Source:**  Adapted of [137]

En está investigación de utilizó la infraestructura de Google Cloud para brindar mayor seguridad a gran parte de las vulnerabilidades mencionadas por Kumar [137].

* + 1. Ataques a Fintech

A lo largo de los años, han existido múltiples 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 peligro a 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, SHA256 [138] 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 “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 [140], en la figura 7 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.

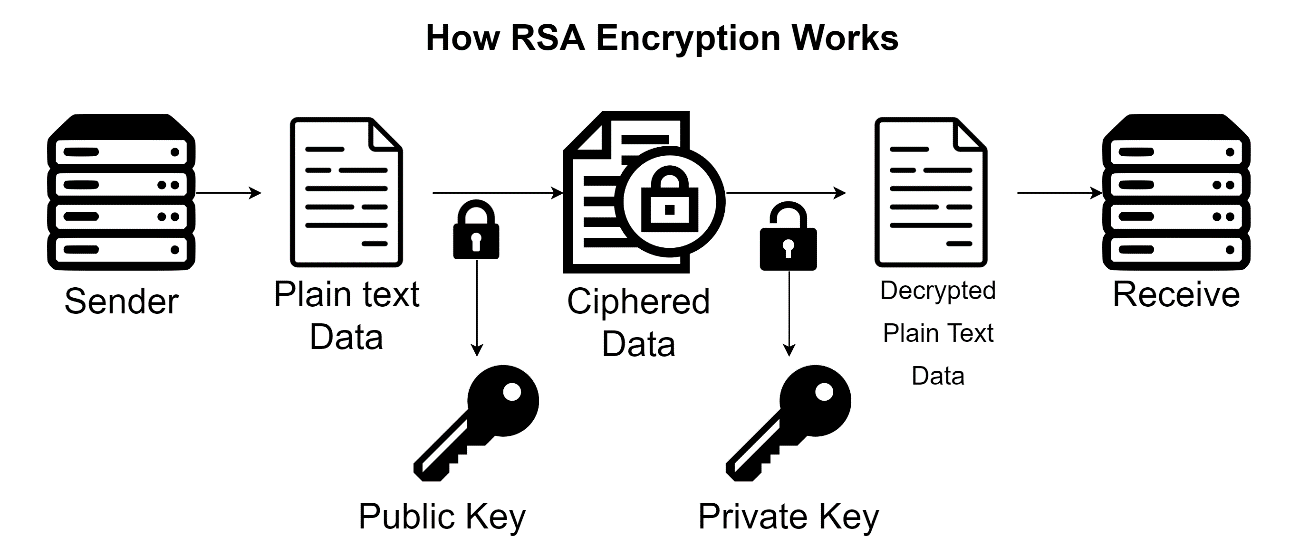


Figure 7: How RSA Encryption Works

***Source:*** *self made*

* + - 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 [142].

La carencia de un doble factor de autenticación en una aplicación Fintech es claramente una vulnerabilidad alta, por eso en esta investigación se implementó una doble autenticación con código PIN o utilizando códigos proporcionados por la aplicación de Google Authenticator [143].

* + - 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 o algoritmos para demostrar el no repudio de los usuarios al momento de utilizar sus tarjetas [144], 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 [145]:

* 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.

Para mitigar fraudes de primera persona, en esta investigación se implementó una verificación biométrica de usuarios para posteriormente convertirlo en una identidad digital con NFT utilizando el estándar ERC-721 y así obtener evidencias que respalden los pagos realizados por estos usuarios dentro de la plataforma en casos de reportarse fraudes.

* + - 1. Estafas al vender o comprar productos online

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.

Para mitigar las estafas producidas en el Marketplace de productos y criptomonedas de la plataforma Fintech Pay2Meta, se implementaron contratos inteligentes con la blockchain de IOTEX utilizando el estándar ERC-20.

* + 1. Metodología Agile Block Chain DApss 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 [164]:

* 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 [165]. 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 [166].

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. 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 de primera persona en aplicaciones Fintech tomando como caso práctico la plataforma Pay2Meta, 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.

* 1. Identidad digital con NFT ERC-721

En la figura 8 se ilustra la propuesta de solución utilizando la verificación biométrica proporcionado por la plataforma MATI en conjunto con smart contract ERC-721 deployados en Iotex para posteriormente crear una billetera de Ethereum que permita pagar las comisiones necesarias para crear el NFT’s con Tatum blockchain y el resultado de esto almacenarlo en IOTA para asegurar su inmutabilidad.

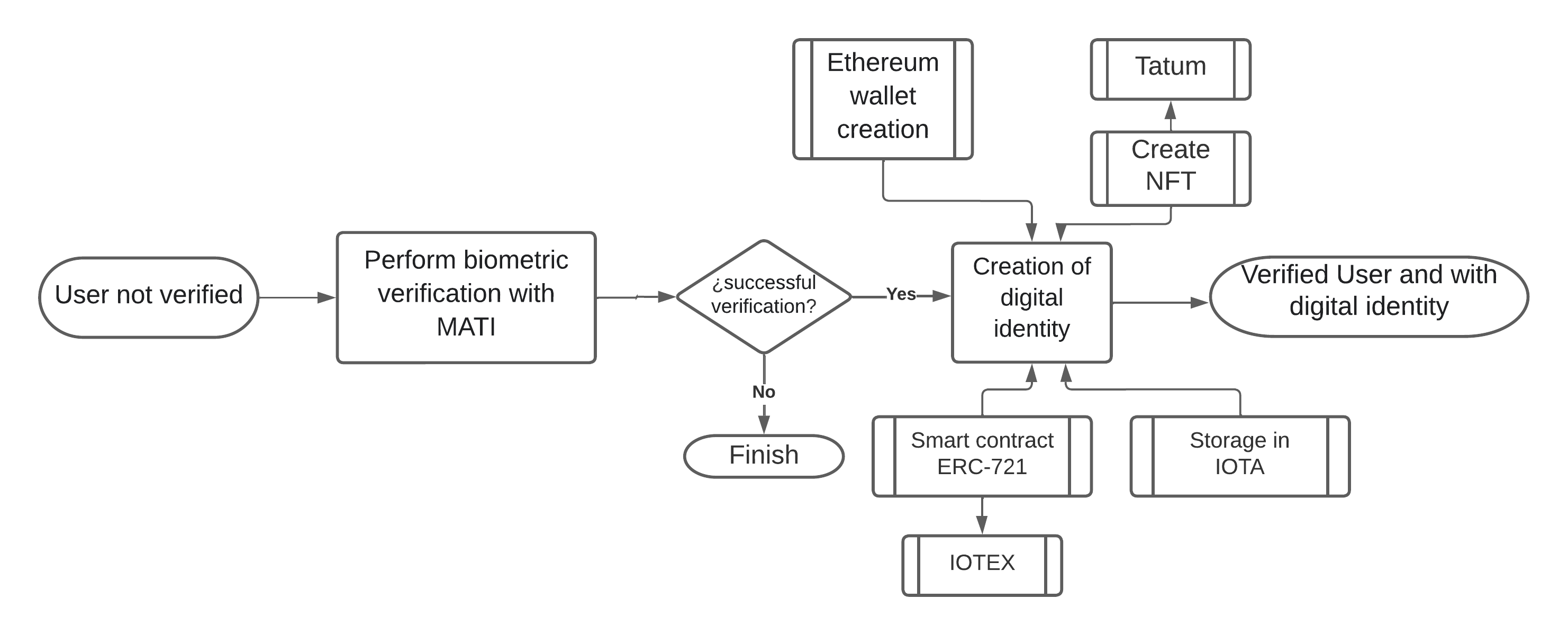


Figure 8: Flowchart of the digital identity process

***Source:*** *self made*

* 1. IOTA y NFT

En la figura 9 se ilustra el proceso de recargar billetera dentro de la plataforma Pay2Meta, partiendo de los usuarios verificados y con identidad digital obtenidos del proceso anterior, cuando realicen la recarga de billetera se les solicitará una doble autenticación con código PIN, huella dactilar o código de Google Authenticator, estos pagos serán encriptados con RSA y se hará uso de IOTA que gracias a su coste cero en sus almacenamientos se guardará la información de estas transacciones financieras como ubicación, IP, dirección, últimas conexiones entre otras informaciones de los usuarios para posteriormente ser utilizado como soporte para defenderse en casos de que existan reclamos de fraude por parte de las entidades bancarias.

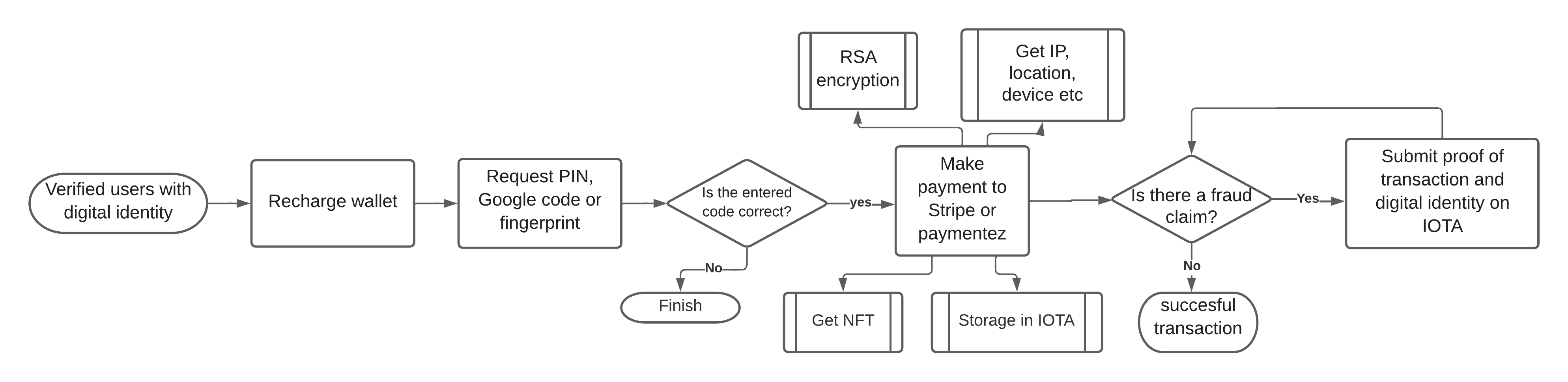


Figure 9: Flowchart of the wallet top-up process

***Source:*** *self made*

* 1. Smart contract ERC-20

En la figura 10 se ilustra la utilización del smart contract ERC-20 para mitigar problemas de estafas cuando se realicen procesos tanto de compras y ventas en el marketplace de productos/servicios como tradings en el marketplace de criptomonedas. Los smart contracts ERC-20 serán deployados con IoTex blockchain y ejecutados con Tatum blockchain y de igual forma los pagos serán encriptados con RSA y las transacciones financieras resultantes serán almacenadas en IOTA.

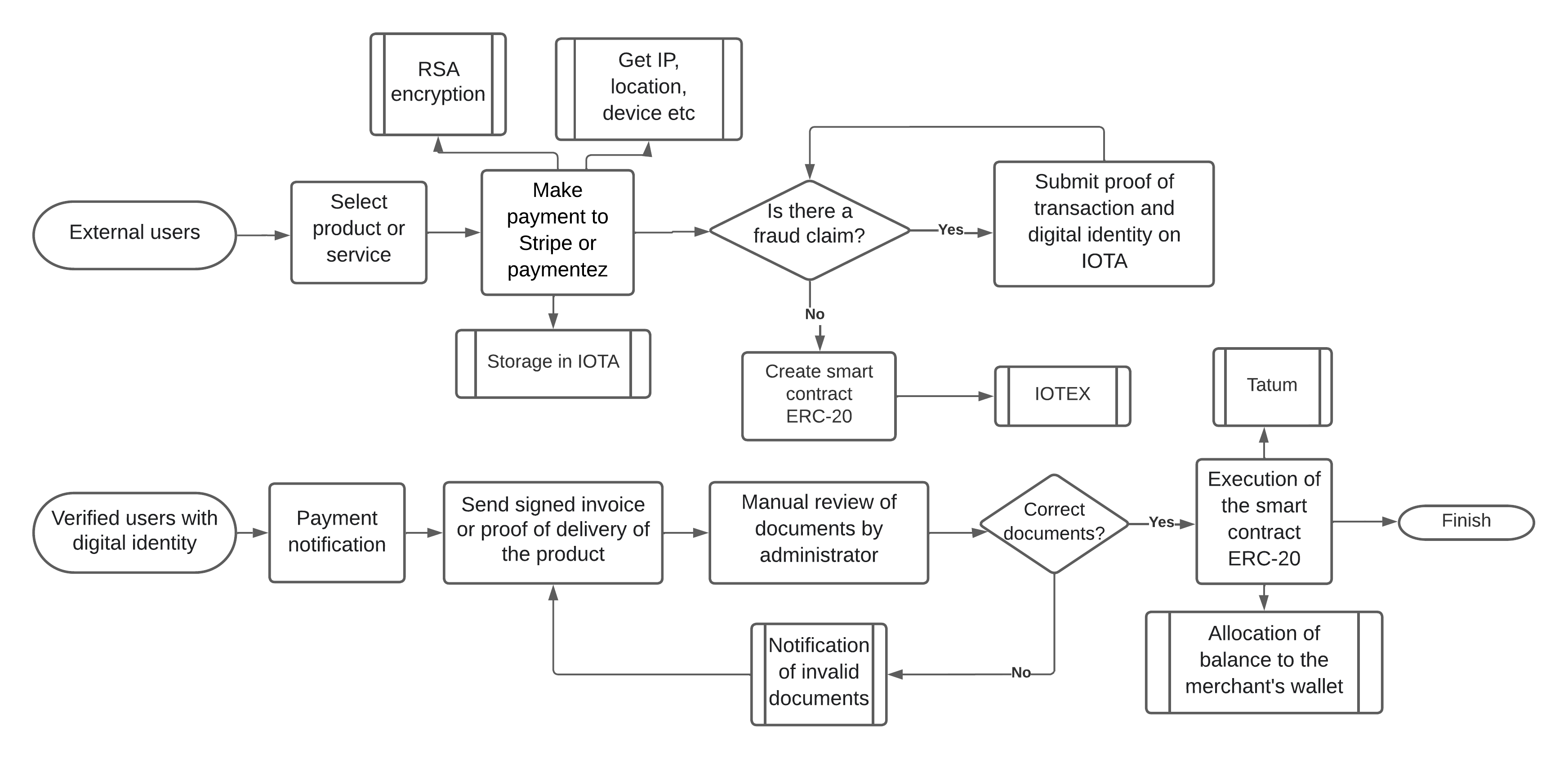


Figure 10: Marketplace process flowchart

***Source:*** *self made*

* 1. Selección de los DLT

Actualmente existen varias plataformas DLT, cada una implementada en diferentes versiones de blockchain (1.0, 2.0 y 3.0) y de Tangle (DAG) ofreciendo diferentes características que podrían ser no ventajosas para ser implementadas en aplicaciones Fintech como comisiones altas, redes privadas, carencia de creación de smart contract o de NFT’s entre otros. Tras una exhaustiva revisión sistemática de literatura usando la guía metodológica de B. Kitchenham se ha podido realizar el siguiente cuadro comparativo ilustrado en la tabla 8 de algunas tecnologías DLT con sus características seleccionadas bajo criterios generales que ayudarían a cumplir con los objetivos propuestos para esta investigación las cuales son las siguientes:

* Tipo de red DLT.
* Madurez de la tecnología.
* Mecanismos de consenso.
* Costos de transacciones
* Aplicabilidad para Smart contract, NFT y Dapps.
* Tiempo de confirmación de transacción.
* Transacciones por segundo
* Descentralización.
* Lenguajes de programación soportado en sus Apis.
* Permisionado.

Tabla 1: DLT Comparison Chart

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Characteristic** | **Distributed Ledger Technologies (DLT)** | | | | | | | |
| **Ethereum** | **IOTA** | **IOTEX** | **TATUM** | **QUORUM** | **HYPERLEDGER FABRIC** | **R3 CORDA** | **XUPER** |
| **Maturity (years)** | High | Medium | Medium | Medium | Medium | High | Medium | Low |
| **Technology** | Blockchain | Tangle | Blockchain | Blockchain | Blockchain | Blockchain | DAG | Blockchain |
| **Consensus mechanism** | Proof-of-work (PoW) | FPC | Roll-DPoS | Depends on the DLT. | Raft-consensus | Proof of Stake | Pluggable consensus | TDPOS |
| **Permissioned** | No | No | No | No | Only validators | Fine permissioned | Strong permissioned | Strong permissioned |
| **Network type** | Public | Public | Public | Public and private | Private and Federated | Private and Federated | Private and Federated | Private and Federated |
| **Smart contracts** | Yes | Yes (Beta Phase) | Yes | Yes | Yes | Yes | Yes | Yes (Beta Phase) |
| **Programming languages** | Solidity | NodeJs, Rust | NodeJS, Go | NodeJS, Python, | Solidity | Go, Python, Java | Kotlin, Java | Java |
| **NFT (tokens)** | Yes | Yes (Beta phase) | Yes | Yes | Yes | Yes | Yes | Yes (Beta phase) |
| **Confirmation time** | 14-15 s | < 10 s | 5 s | < 5 s | 4 a 10 s | 5 a 10 s | 5 a 10 s | 2 a 5 s |
| **CPT (costs)** | 21.000 gas | $0.00 | $0.01 | Depends on the DLT. | $0.20/h | $0.15/h | $0.665/h | $0.15/h |
| **TPS (transactions)** | -20 TPS | 1000 TPS | 2000 TPS | -100 TPS | -100 TPS | >2000 TPS | -170 TPS | 10.000 TPS |
| **Dapps** | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| **Decentralization** | Yes | Yes (Beta phase) | Yes | Yes | Yes | Yes | Yes | No |

* 1. Aplicación de la metodología ABCDE

Según lo detallado por el autor Tonelli [146] acerca del proceso de la metodología ABCDE, los pasos para el desarrollo de sistemas Dapps son los siguientes:

* + 1. Definición del objetivo del sistema

Implementar tecnologías de registros distribuidos en una arquitectura de microservicios de Google Cloud utilizando Blockchain, Tangle y la metodología ABCDE para incrementar la probabilidad de ganar disputas financieras en casos de estafas y fraudes de primera persona realizadas en transacciones financieras online de una aplicación Fintech.

* + 1. Identificación de actores.

Se identificó un total de cuatro actores los cuales fueron:

* Clientes registrados.- Son usuarios registrados dentro del sistema, hacen uso de las diferentes funcionalidades del sistema interactuando como clientes.
* Comercios registrados.- Son usuarios registrados dentro del sistema, pero se diferencia de los clientes debido a que los comercios generan ganancias en los marketplaces.
* Usuarios externos.- Son usuarios que no pertenecen a la plataforma, pero realizan pagos a través de links de cobros generados por usuarios registrados.
* Sistema.- Es toda la arquitectura informática vista como un sistema, encargada de ejecutar eventos, enviar notificaciones, ejecutar smart contracts entre otras funcionalidades.
  + 1. Definir casos de usos y diagrama de clase.

Una vez identificado a los actores y realizado las historias de usuarios correspondientes, el siguiente paso fue diseñar los casos de usos. En la figura 11 se ilustra el caso de uso unificado, el mismo que está elaborado con los actores mencionados anteriormente con sus respectivos sub sistemas que corresponden al backoffice donde se realiza las recargas de billeteras con tarjetas de créditos de usuarios registrados, el subsistema de marketplace donde se realizan compras y ventas de productos y criptomonedas y finalmente el subsistema de links de pagos donde se realizan pagos con tarjetas de créditos de usuarios externos a la plataforma.

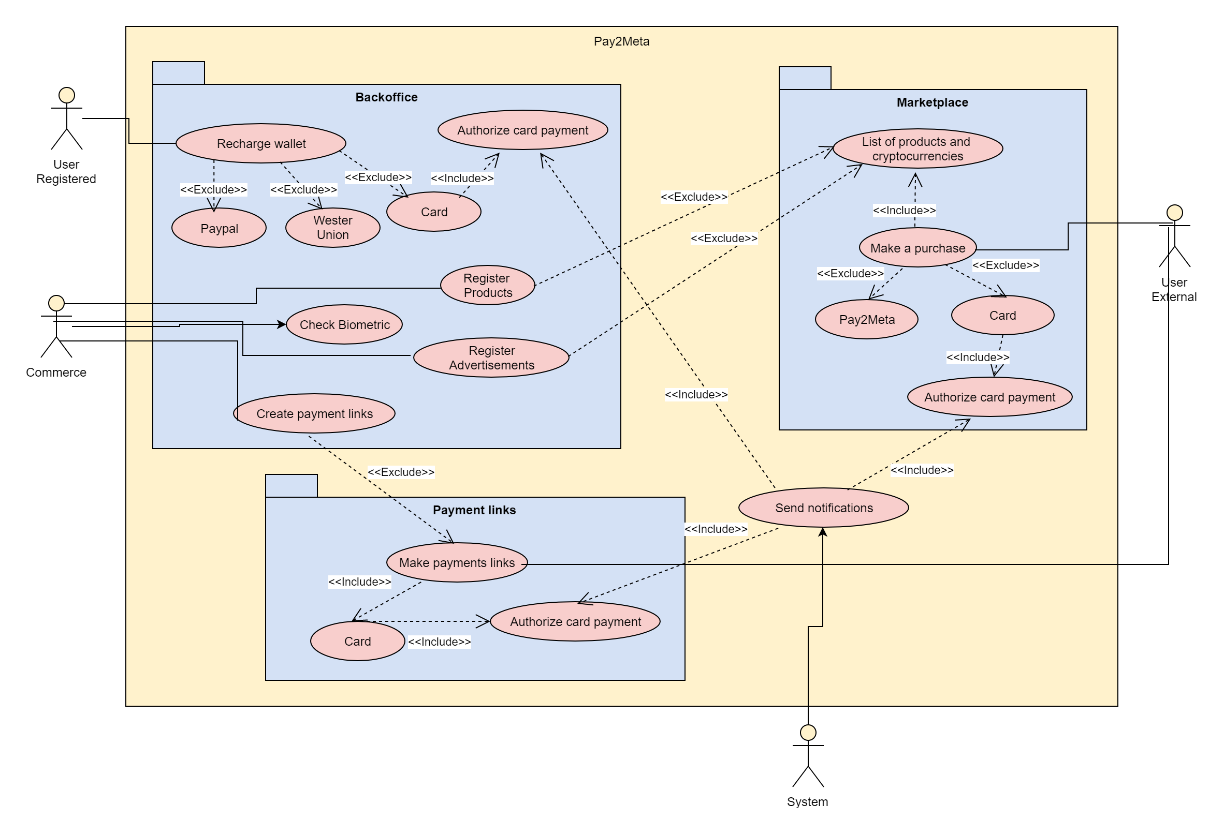


Figure 11: Unified use case

Finalmente, se elaboró el diagrama de clases tal y como se ilustra en la figura 12, el mismo que está conformado por clases como smart contracts, usuarios, compras y ventas

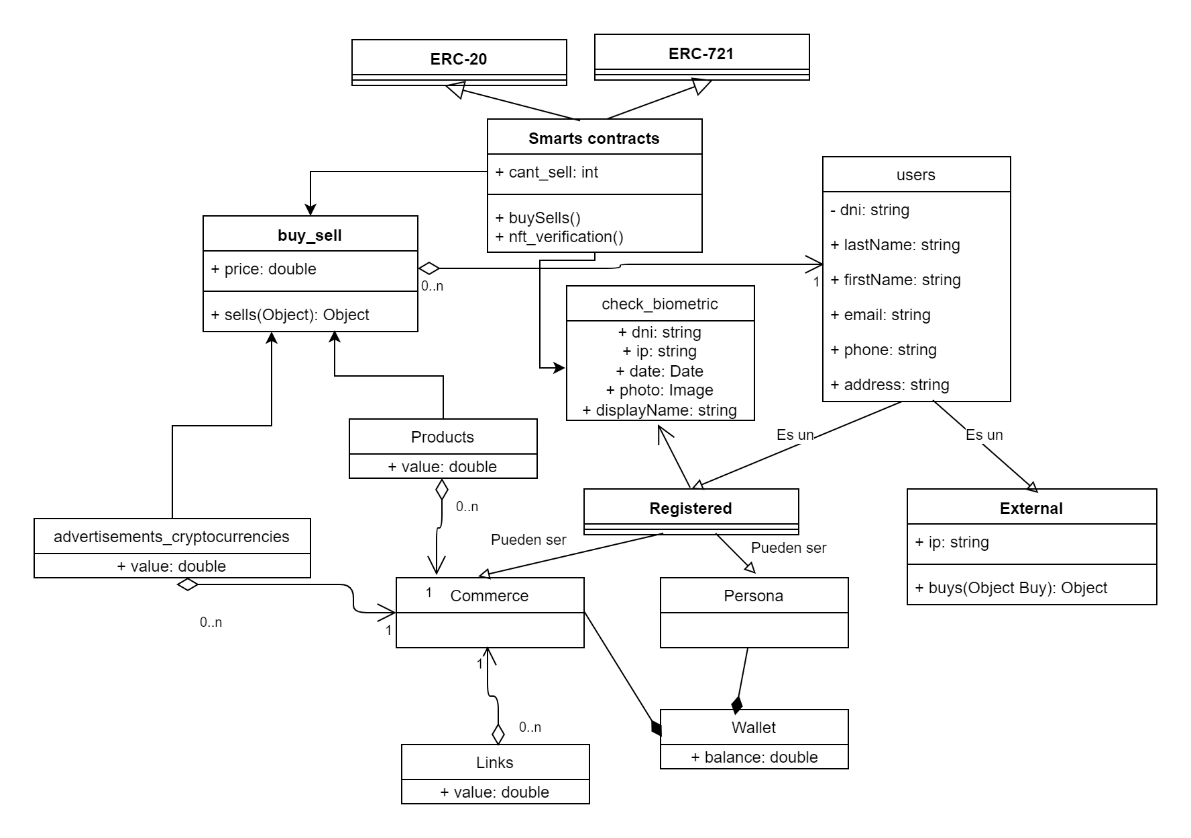


Figure 12: Class diagram

1. Caso de estudio: Fintech Pay2Meta

4.1 Arquitectura general

La arquitectura utilizada fue una de microservicios usando Google Cloud, en la figura 13 se ilustra el diseño utilizado, el cual consta de varias aplicaciones clientes entre móvil y web, además todos los datos provenientes de estas aplicaciones clientes serán encriptadas con RSA hacia los api Gateway el mismo que se encargará de balancear y distribuir las peticiones https hacia los diferentes microservicios, estos microservicios se encargarán de desencriptar la información y volverla a encriptar con AES usando las llaves privadas obtenidas de la base de dato criptográfica de IOTA Stronghold para posteriormente almacenar la información en diferentes base de datos relacionales y no relacionales. Finalmente, estos microservicios realizarán envíos de notificaciones utilizando el balanceador de carga y cloud pub/sub de Google; y también conexiones con plataformas externas como Stripe, Paymentez; almacenamientos en IOTA y elaboración de smart contracts con Iotex y Tatum.

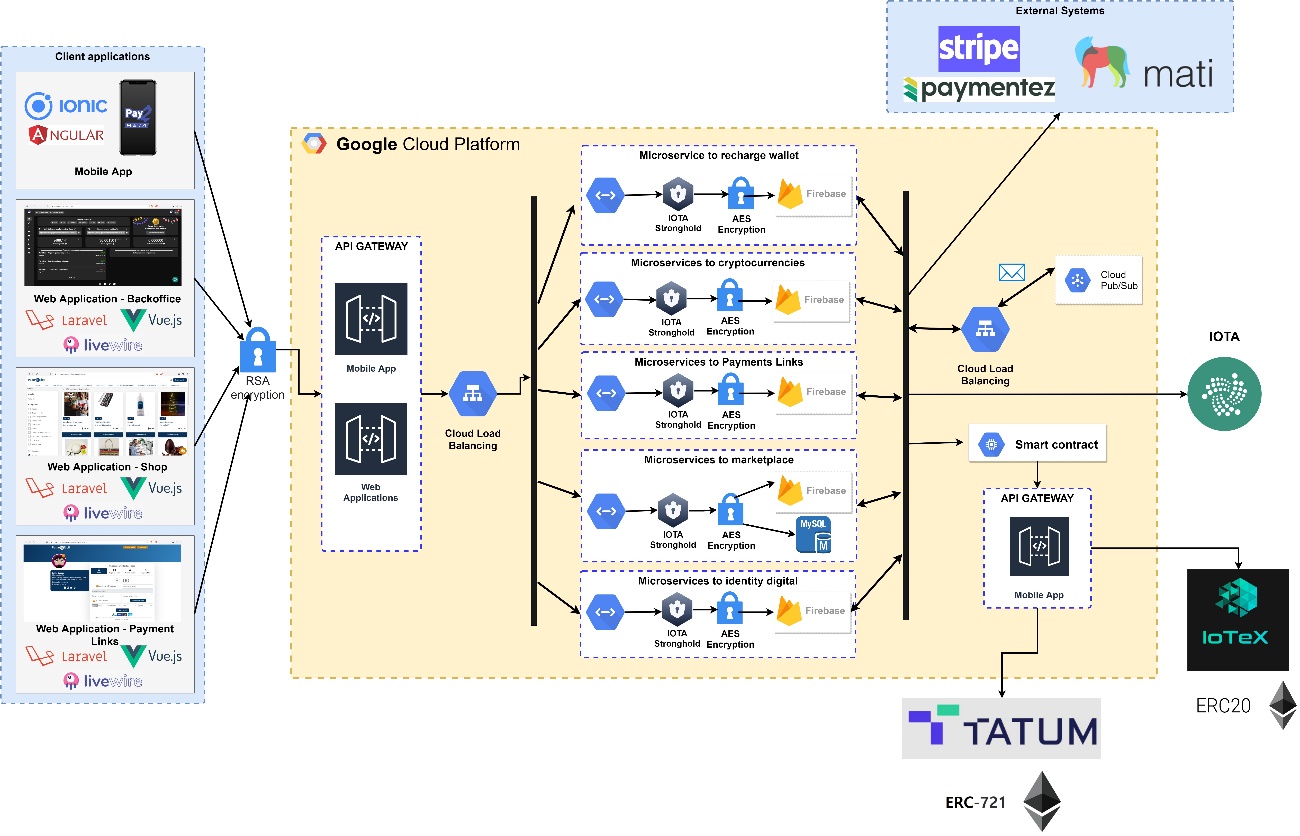


Figure 13: Pay2Meta architectural design

4.2 Microservicios

En la figura 14 se ilustra la utilización de dos instancias de tipo Google Cloud Engine para el almacenamiento de las aplicaciones web correspondientes al backoffice y al Marketplace que internamente también se configuraron manejo de eventos y notificaciones para las diferentes aplicaciones Fintech Pay2Meta.

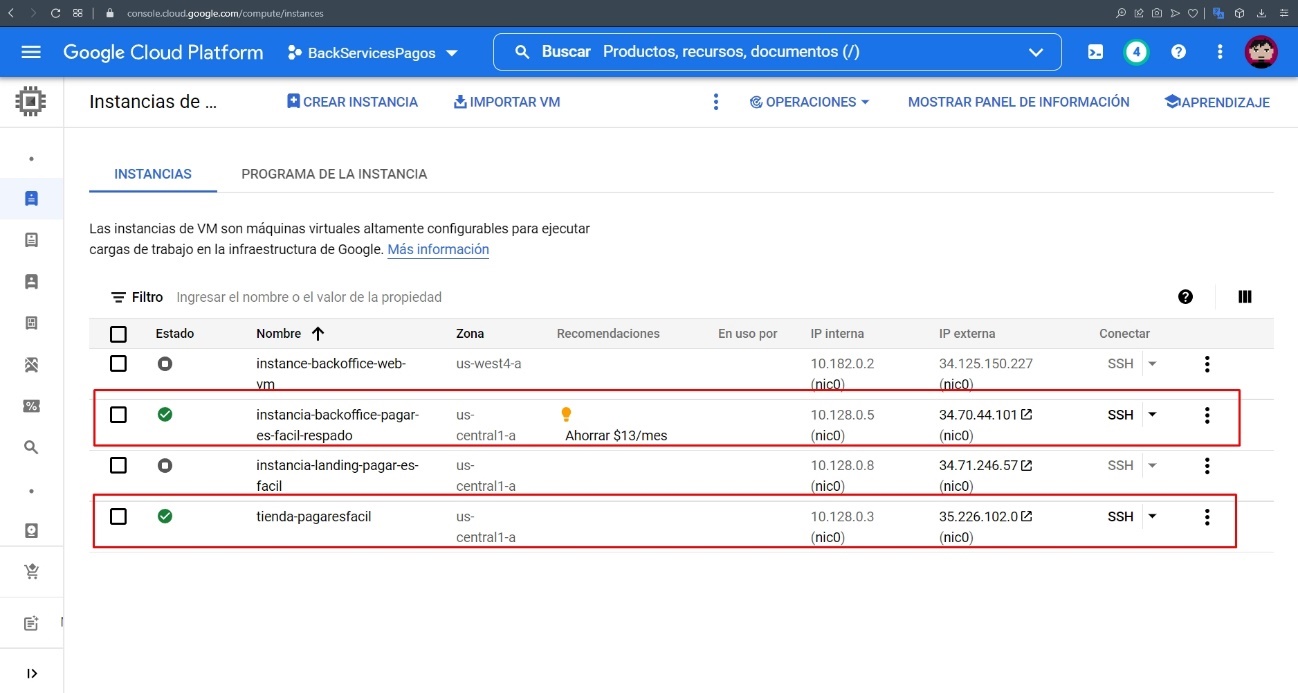


Figure 14: Instance Google Cloud

En cuestión de los microservicios, en la figura 15 se ilustra la implementación de endpoints utilizando Firebase functions de tipo https, entre ellas se destaca el endpoint “consultas2” utilizado para funcionalidades generales de las aplicaciones como pagos, transacciones, consultas etc y el endpoint “cryptos” utilizado para las funcionalidades correspondientes a los DLT como son los contratos inteligentes, NFT y pagos con criptomonedas. En la figura 15 también se destacan las extensiones de tipo Firebase Bigquery para la realización de consultas por lotes (batch). Cabe recalcar que estos microservicios fueron implementados en NodeJS 16, NPM 6.14.10 y Firebase 10.8.0.

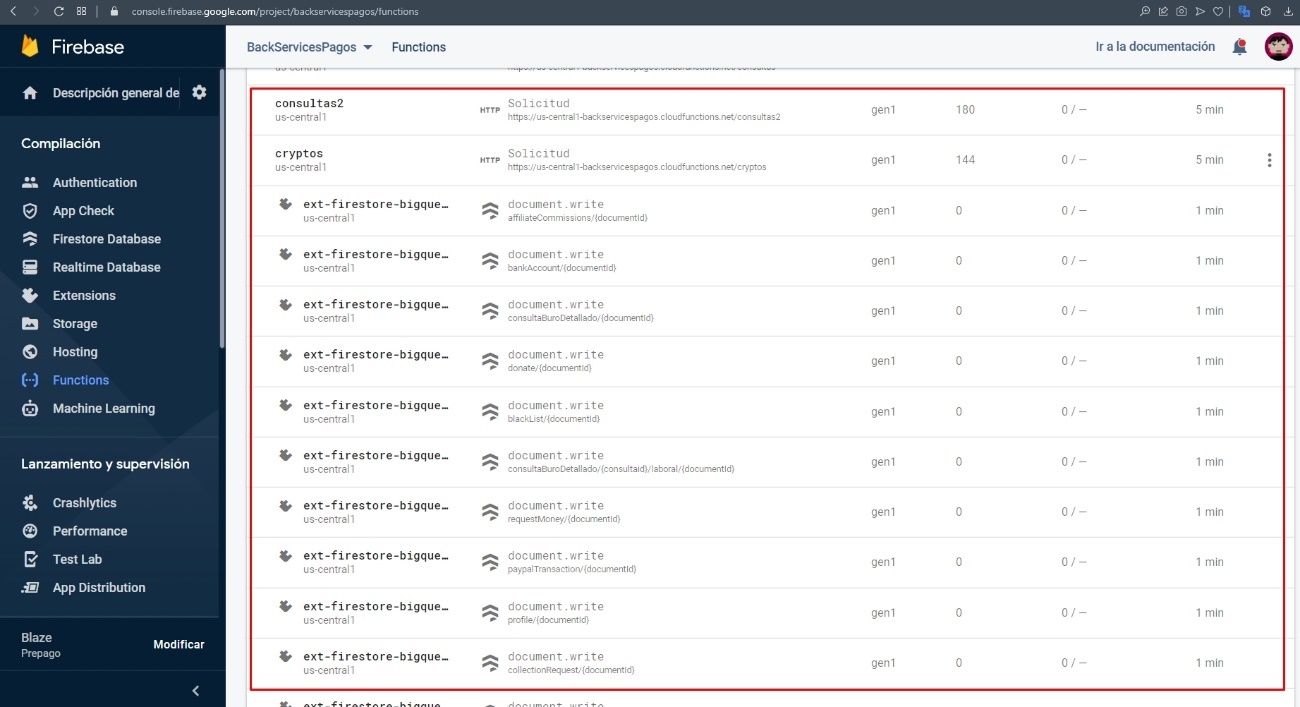


Figure 15: Https endpoint and bigquery extensions with Firebase Functions

Con respecto a IOTA, en la figura 16 se ilustra el endpoint de tipo https llamado “iota” utilizado para las funcionalidades donde involucren almacenamientos en IOTA, también existe una función de tipo Cloud Firestore llamado “notification” utilizado para el envío de notificaciones que se ejecutarán automáticamente cuando los usuarios terminen de realizar pagos y finalmente funciones de tipo Cloud/Pub programadas para que se ejecuten cada cierto tiempo y realizar alguna tarea en específica.

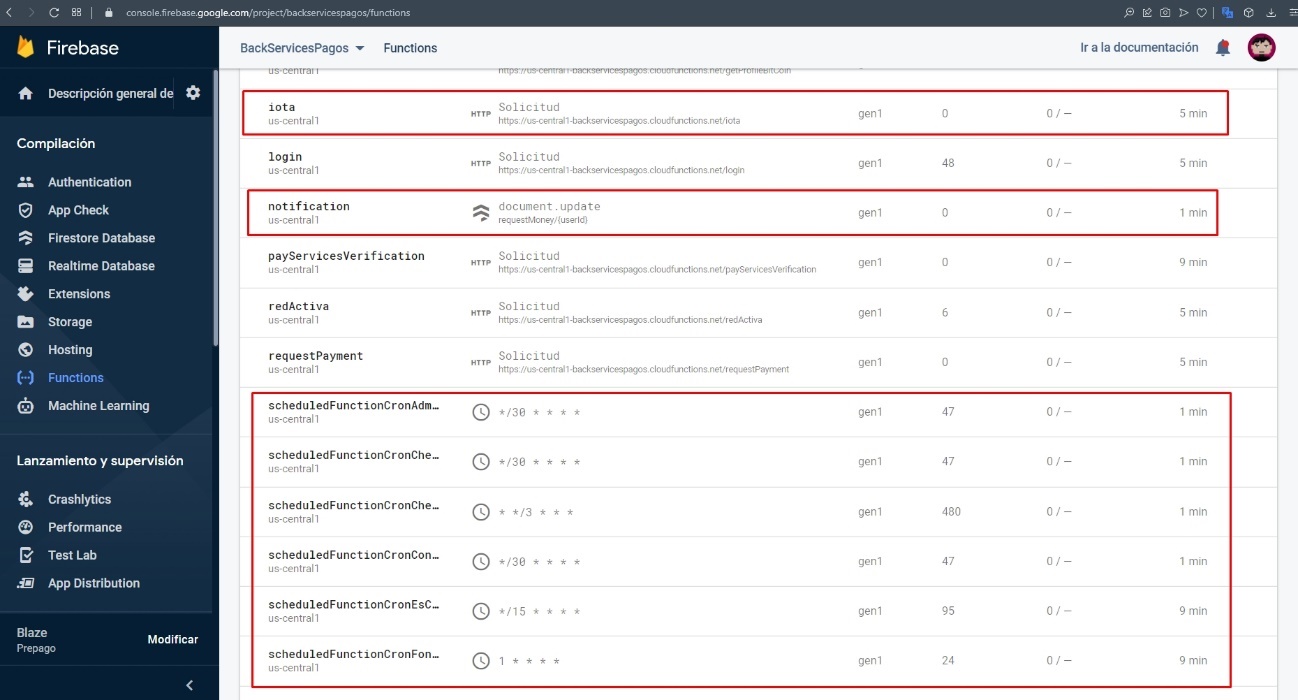


Figure 16: IOTA endpoint https, notification with Cloud Firestore and Cloud Pub/Sub

Otros de los microservicios relevantes implementados en esta investigación fueron los triggers de tipo Cloud Firestore, en la figura 17 se ilustra los diferentes triggers que se ejecutarán dependiendo de los cambios que se realicen en los documentos de Firebase por las acciones de los usuarios en las aplicaciones clientes.



Figure 17: Triggers with Cloud Firestore

4.3 Frontend interfaz de usuario

A continuación, se presenta las interfaces más importantes realizadas en las diferentes funcionalidades y artefactos. La aplicación móvil ilustrada en la figura 18 fue realizada con el framework Angular 12 e IONIC 5.

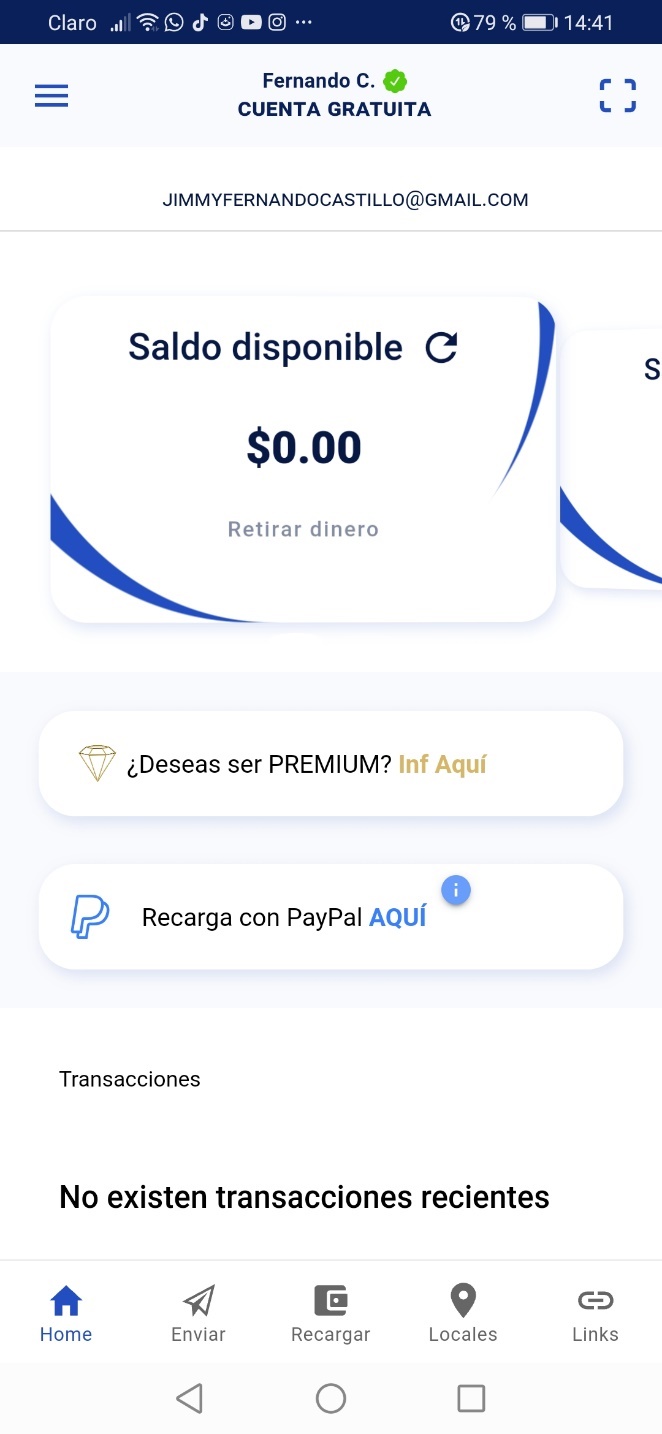


Figure 18: Mobile App Pay2Meta

La funcionalidad de links de pagos ilustrada en la figura 19 fue implementada en una instancia de Google Cloud y desarrollado con el framework Laravel 8 como tecnología backend, los frameworks Livewire 2 y VueJS 3 como tecnología frontend y Firebase y Mysql como bases de datos.

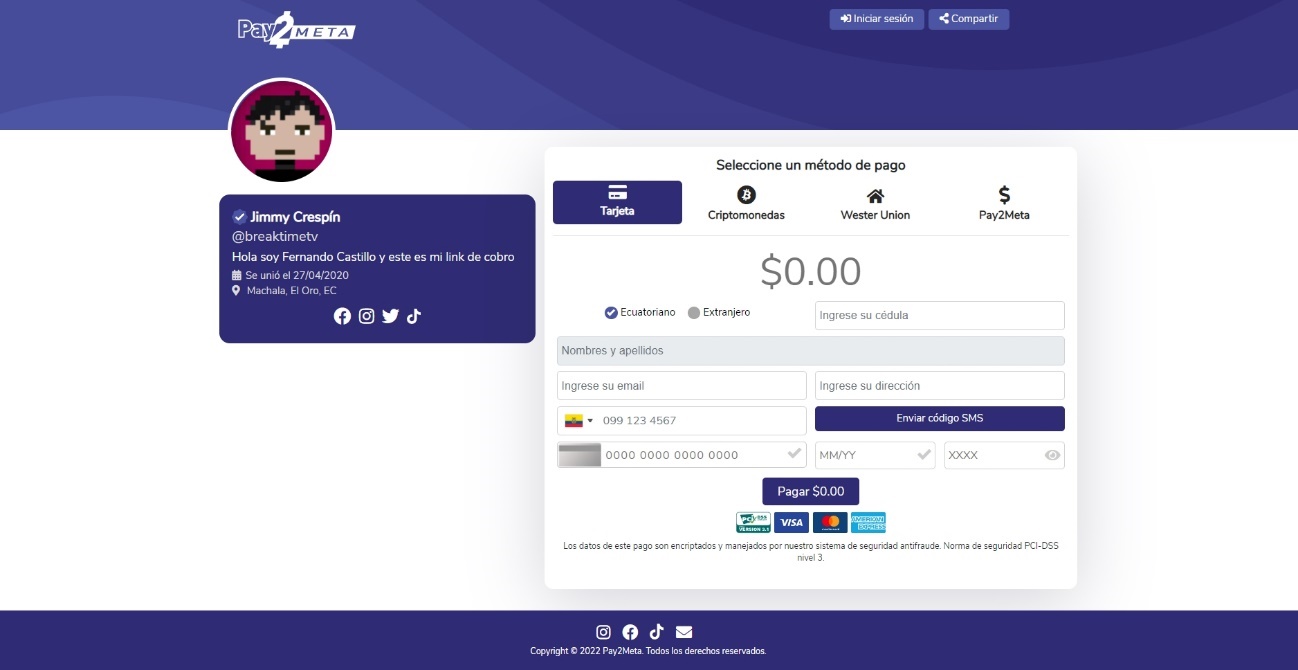


Figure 19: Functionality Payments Links

El artefacto del backoffice ilustrada en la figura 20 fue implementada igualmente en una instancia de Google Cloud con el framework Laravel 8 como tecnología backend, los frameworks Livewire y VueJS 3 como tecnología frontend y firebase como base de datos. En esta ventana los usuarios realizan las recargas de billeteras para tener saldo dentro de la plataforma.

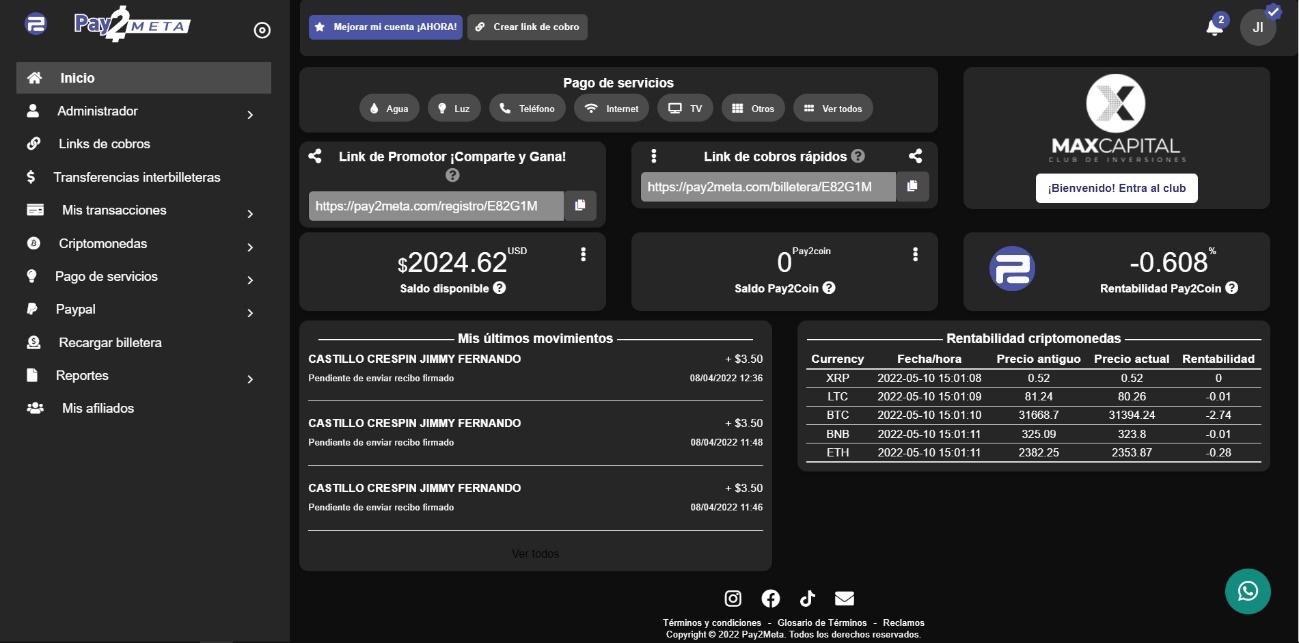


Figure 20: Web Application Backoffice Pay2Meta

El artefacto del trading con criptomonedas ilustrada en la figura 21 fue realizada con el framework Laravel 8 como tecnología backend, los frameworks Livewire y VueJS como tecnología frontend, firebase como base de datos y Tatum como tecnología DLT.

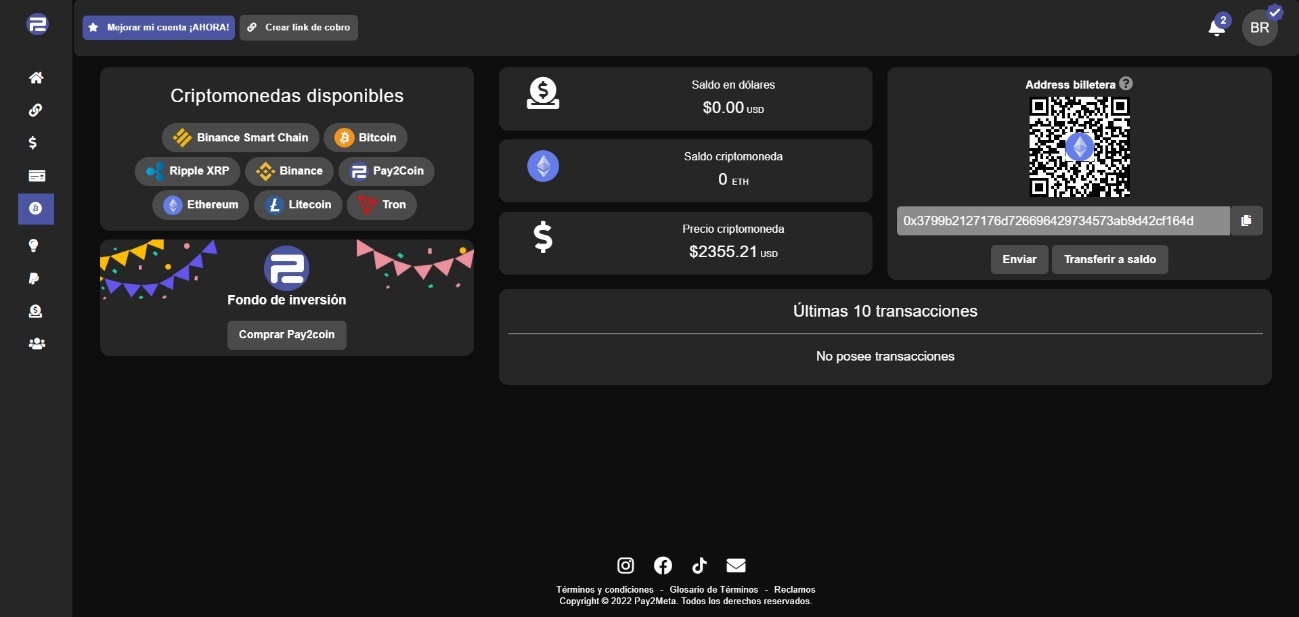


Figure 21: Web Application Marketplace Cryptocurrencies

4.4 Backend diagrama de procesos

Fueron tres diagramas de procesos elaborados en esta investigación, el primero se ilustra en la figura 22 el cual consiste en el proceso de verificación biométrica de los usuarios, para eso se utiliza un sistema externo llamado Mati. Cuando termina la verificación, se procede a crear un QR de los datos del perfil del usuario verificado y esta imagen posteriormente se convertirá en una identidad digital utilizando un smart contract con Iotex y NFT’s de la plataforma Tatum y el resultado de esto se almacenará en IOTA para asegurar su inmutabilidad. Cabe recalcar que, para realizar está identidad digital, los usuarios previamente deberán tener una billetera de criptomoneda de Ethereum, la misma que se puede crear en la plataforma Fintech estudiada y esta billetera deberá tener al menos un saldo de 5 centavos en ether para deployar el smart contract en Iotex.

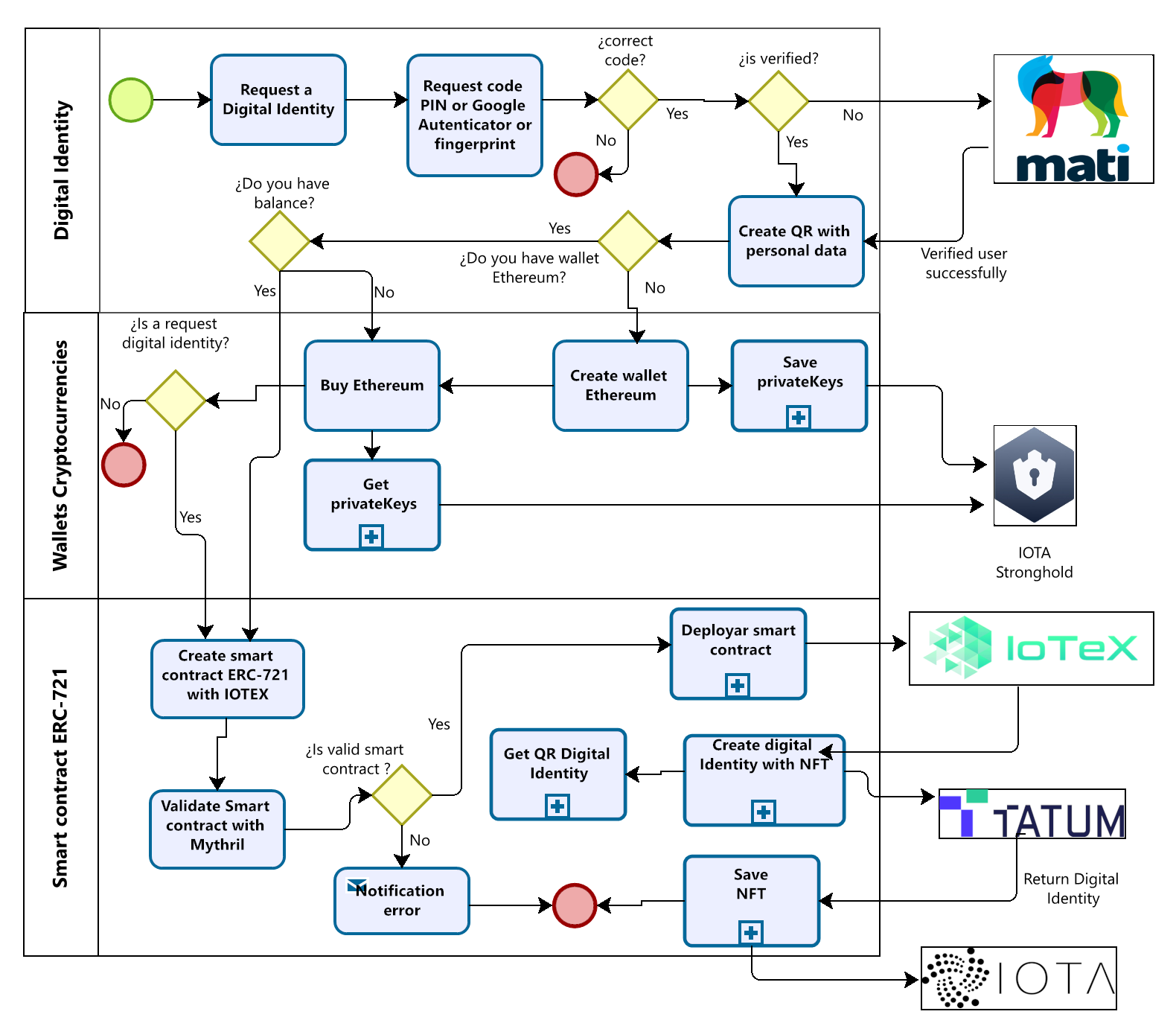


Figure 22: Digital Identity with NFT

El segundo proceso ilustrado en la figura 22 es acerca de la funcionalidad de recargar billetera ofrecida por la aplicación Fintech estudiada en esta investigación. Esta funcionalidad fue escogida por el motivo de que involucra pagos con tarjetas de crédito o débito de los usuarios verificados biométricamente para utilizar los NFT’s creados anteriormente y en conjunto con los datos de la transacción almacenadas en IOTA; tratar de ganar las disputas financieras provocados por fraudes ofreciendo está información adicional a los bancos.

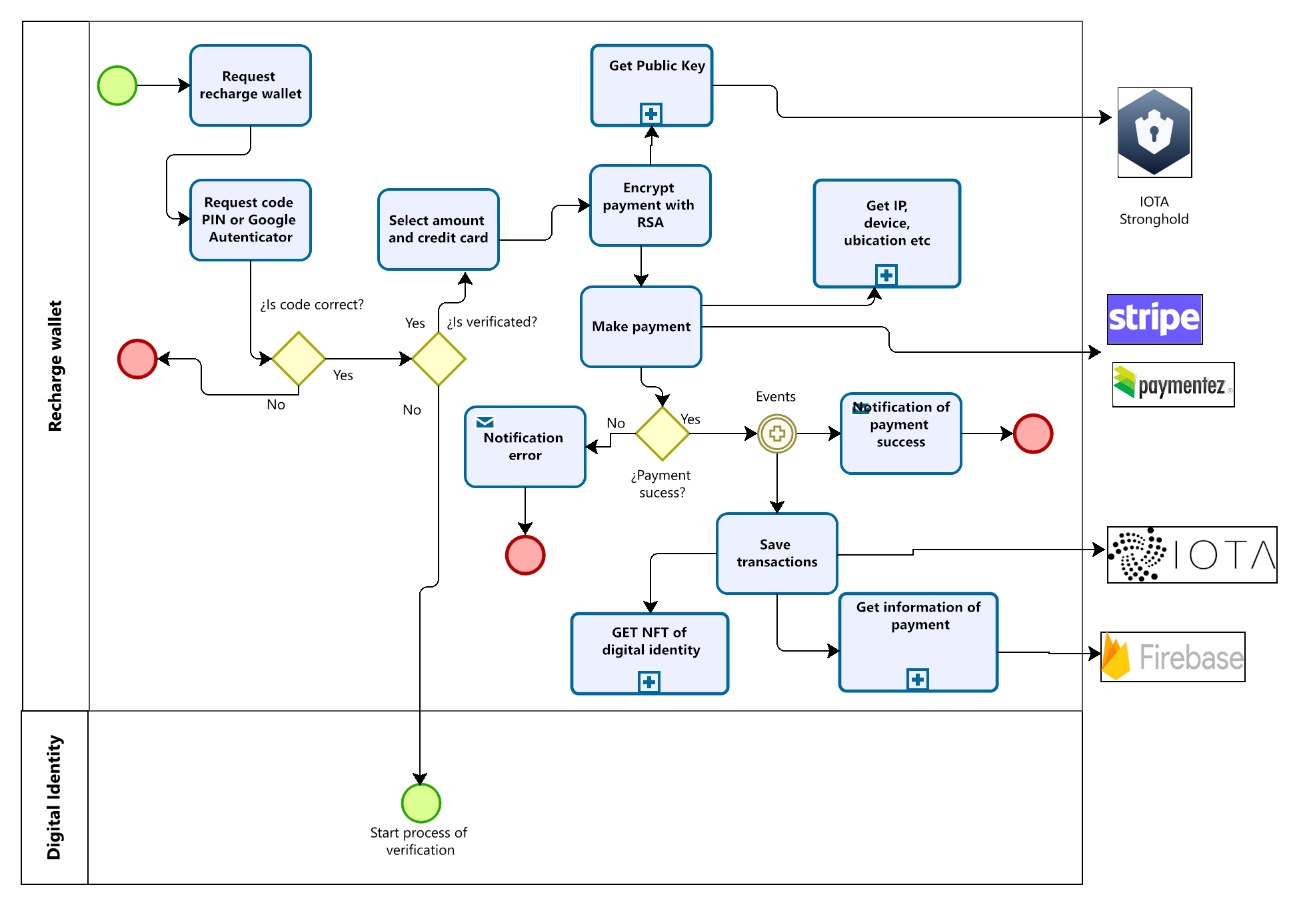


Figure 23: Process of recharging wallet with NFT and IOTA

Finalmente, el tercer proceso ilustrado en la figura 24 es acerca de la funcionalidad de links de cobros y marketplace ofrecidas por la aplicación Fintech estudiada en esta investigación. Estas funcionalidades fueron escogidas por el motivo de que involucran a usuarios externos que no poseen una identidad digital. Para esta solución se utilizó contratos inteligentes ERC-20 donde el comercio deberá enviar al administrador de la plataforma algún documento firmado por parte del usuario que realizó la compra, que indique que el producto vendido haya sido enviado al cliente. Una vez que se cumpla con este acuerdo, el contrato inteligente se ejecutará y se depositará el dinero en criptomonedas al comercio. La transacción resultante se almacenará en IOTA para asegurar su integridad e inmutabilidad.

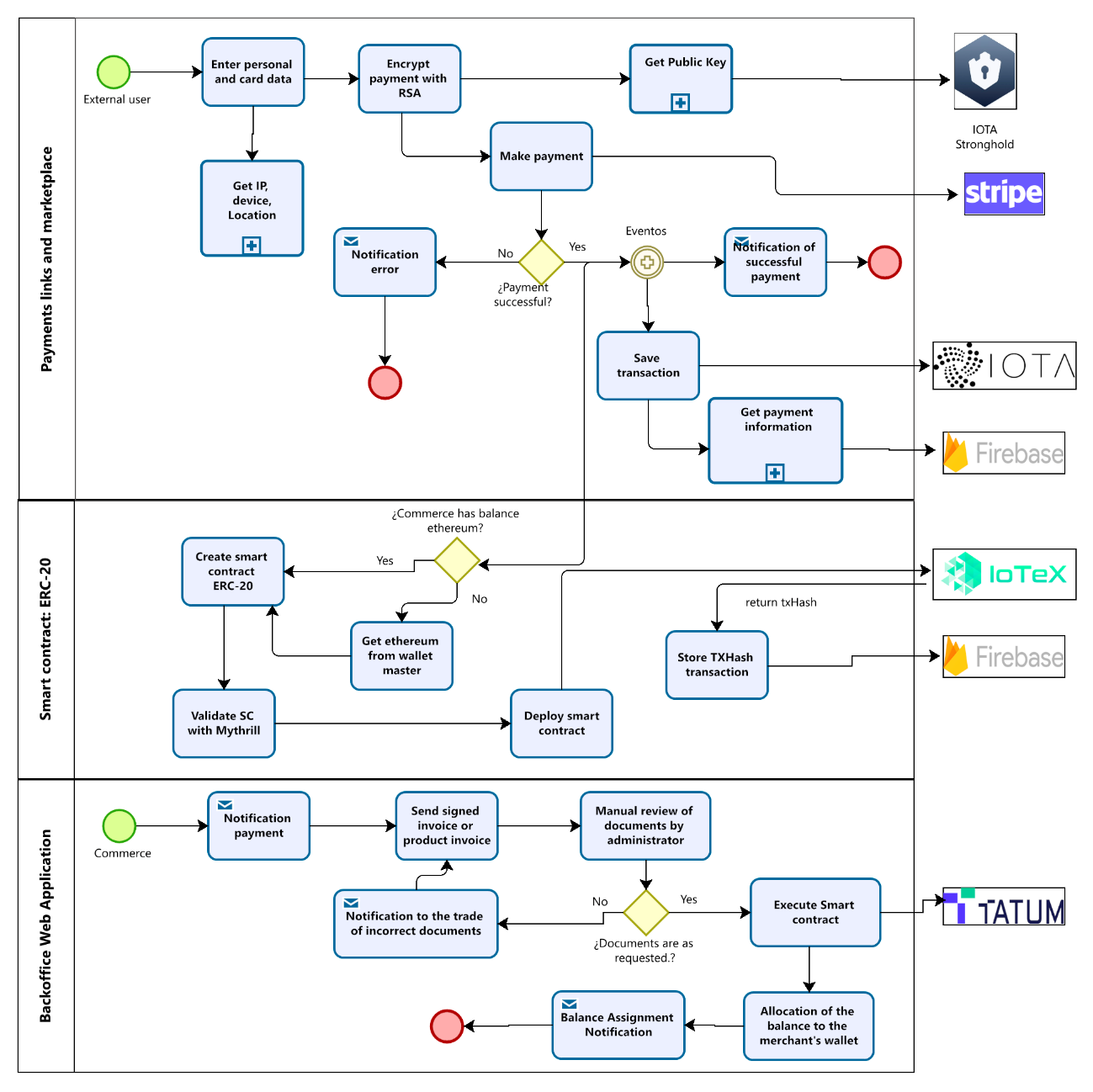


Figure 24: Buying - selling process on Marketplace

4.5 Subsistemas DLT

Para el registro de transacciones de coste cero con IOTA se utilizó el código de programación ilustrada en la figura 25 donde se detallan aspectos como la ip, características del dispositivo, coordenadas de ubicación, nombre del navegador, sistema operativo, fecha, hora, userId y la cantidad de la transacción que el usuario realizó en la plataforma Fintech Pay2Meta. Estos datos servirán posteriormente como prueba transaccional inmutable en caso de reportar fraude por parte de la entidad bancaria.

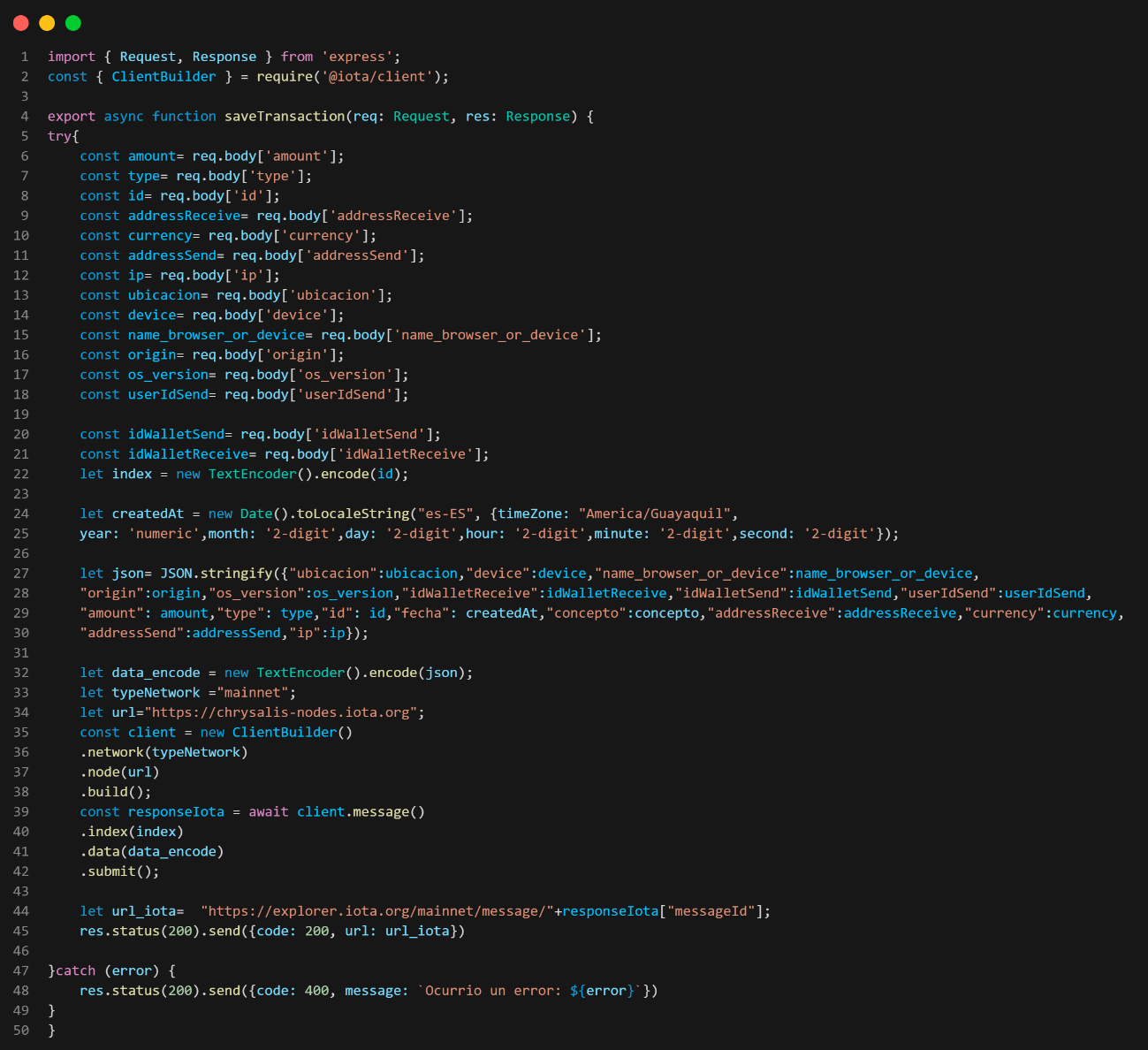


Figure 25: Programming code to store a transaction in IOTA

Con respecto a los smart contract ERC-20 se utilizó el lenguaje de programación solidity, en la figura 26 se ilustra una porción del código utilizado para las transferencias de criptomonedas de Ethereum cuando se cumple los acuerdos establecidos por el comercio y los compradores en los marketplaces de productos y de criptomonedas disponibles en la aplicación Fintech Pay2Meta.

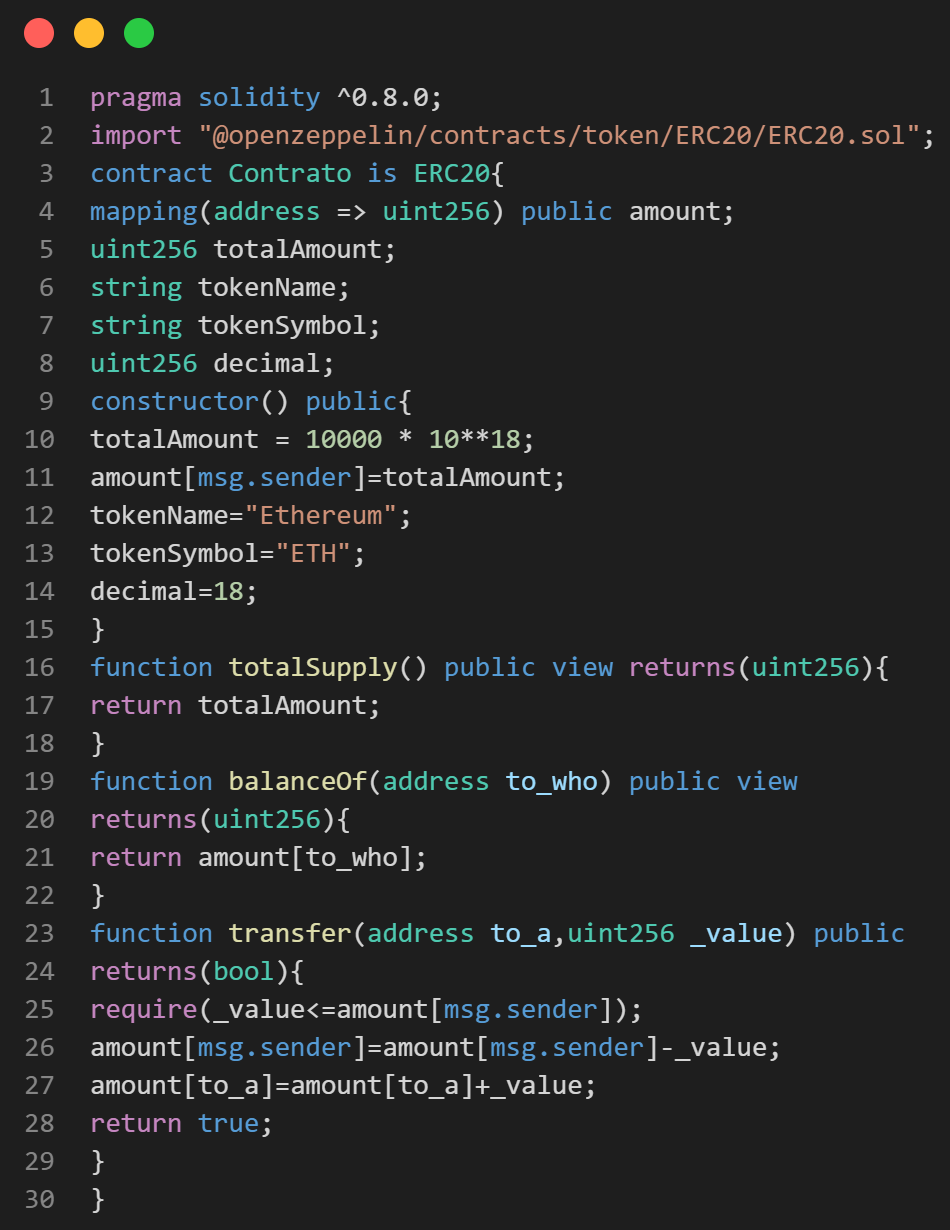


Figure 26: Programming code for smart contract ERC-20

Con respecto a los smart contract ERC-721 se utilizó el lenguaje de programación python, en la figura 27 se ilustra una porción del código utilizado para la creación del NFT el cual obtiene de un archivo json todos los IPFS con las imágenes de los códigos QR de la identidad digital de los usuarios.

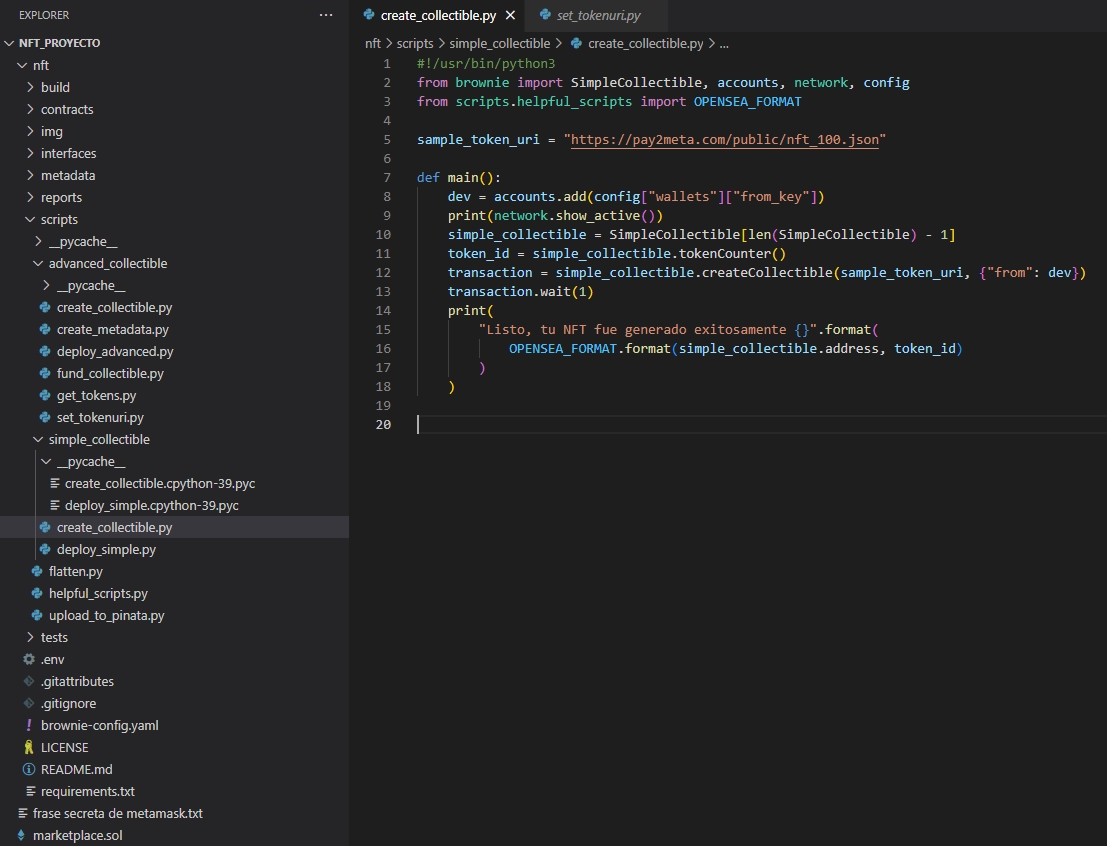


Figure 27: Programming code for smart contract ERC-721 in Python

1. **Experimentos**

Entre los experimentos que se realizaron se encuentra el experimento setup que detalla el entorno donde se realizaron las pruebas junto con las herramientas y dispositivos que se utilizaron especificando las características principales de cada una de ellas. Las pruebas de funcionamiento donde se demuestra que el sistema funciona tal y como fue diseñado, las pruebas de seguridad donde se demuestra que el sistema diseñado es seguro, las pruebas de rendimiento que demuestran que los DLT seleccionados son óptimos en tiempos de respuestas para ser utilizados en aplicaciones Fintech y pruebas de latencia para conocer el tiempo de ejecución entre microservicios durante los pagos.

**5.1 Experimental setup**

La siguiente investigación se lo realizó en un ambiente de producción controlado, tomando como caso práctico las transacciones realizadas por los usuarios en las funcionalidades de links de cobros, Marketplace de criptomonedas y recargas de billetera ofrecidas por la plataforma Fintech “Pay2Meta” que requiere de la implementación de los DLT en sus procesos financieros mencionados anteriormente para incrementar la seguridad de los datos transaccionales y a su vez mitigar los problemas de fraudes/estafas de primera persona detectadas en las funcionalidades del 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.

Para las pruebas de rendimiento se utilizó una computadora personal como cliente, con las características mostradas en la tabla 2, donde se detallan el procesador, la memoria RAM y el sistema operativo.

|  |  |
| --- | --- |
| CPU | AMD Ryzen 7 3200 2.30 Ghz |
| RAM | 16 GB |
| Operating System | Windows 11 |

Tabla 2: Characteristics of equipment for local performance tests

En cuestión de los microservicios con cloud functions, en la tabla 3 se ilustra las características del servidor utilizado, donde se especifican aspectos como la región donde se encuentra, el entorno de ejecución, la memoria y el tiempo máximo de espera en ejecución.

|  |  |
| --- | --- |
| Server region | us-central1 |
| Runtime environment | NodeJS 16 |
| Memory | 1 GB |
| Maximum waiting time in execution | 5 minutes |

Tabla 3: Google Cloud Functions server features

Con respecto al servidor donde se encuentran alojado los proyectos clientes como la plataforma web del backoffice y marketplace, en la tabla 4 y figura 65 se ilustran las características del mismo donde se especifica la ubicación del servidor, que tipo de máquina se utilizó, la cantidad de CPU virtual utilizada, así como el tamaño de la memoria y disco duro.

|  |  |
| --- | --- |
| Server location | us-central1-a |
| Machine type | G1-small |
| Number of virtual CPUs | 4 CPU virtuals |
| Memory | 4 GB |
| HDD | 20 GB |

Tabla 4: Google Cloud Platform server features

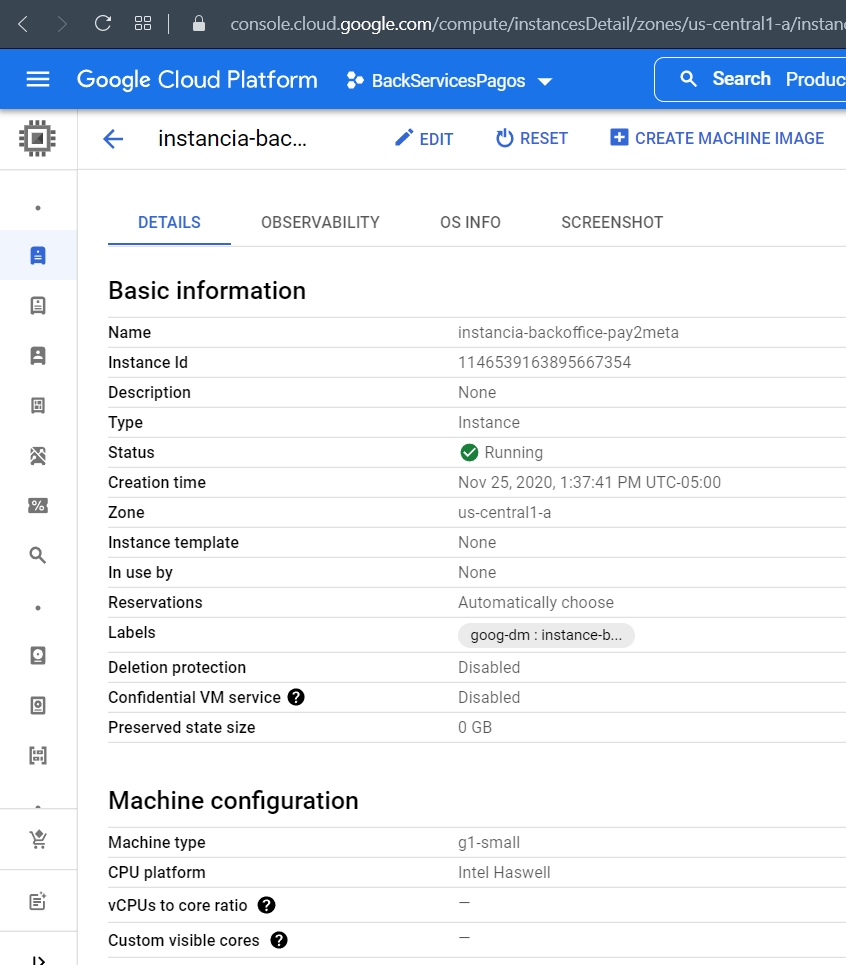


Figure : Characteristics of the server used in Google Cloud

Las herramientas seleccionadas se encuentran dividido en tres grupos tal y como se ilustra en la figura 29, el primer grupo será utilizado para el análisis de datos, siendo seleccionada la herramienta Excel y validándolo con SPSS (<https://www.ibm.com/analytics/spss-statistics-software>) . El segundo será utilizado para la recolección de datos, en este grupo se encuentran bases de datos como Firebase y Mysql de donde se obtendrán los registros transaccionales. El tercer grupo está enfocado a la realización de pruebas donde se encuentra JMeter (https://jmeter.apache.org/download\_jmeter.cgi) que será utilizado para realizar pruebas funcionales, testeo de aplicaciones y servicios web; Postman (<https://www.postman.com/downloads/>) para testeo de endpoints, wireshark (https://www.wireshark.org/download.html ) para el análisis de paquetes y Pay2Meta (<https://pay2meta.com>) donde los usuarios utilizaron las funcionalidades del sistema.

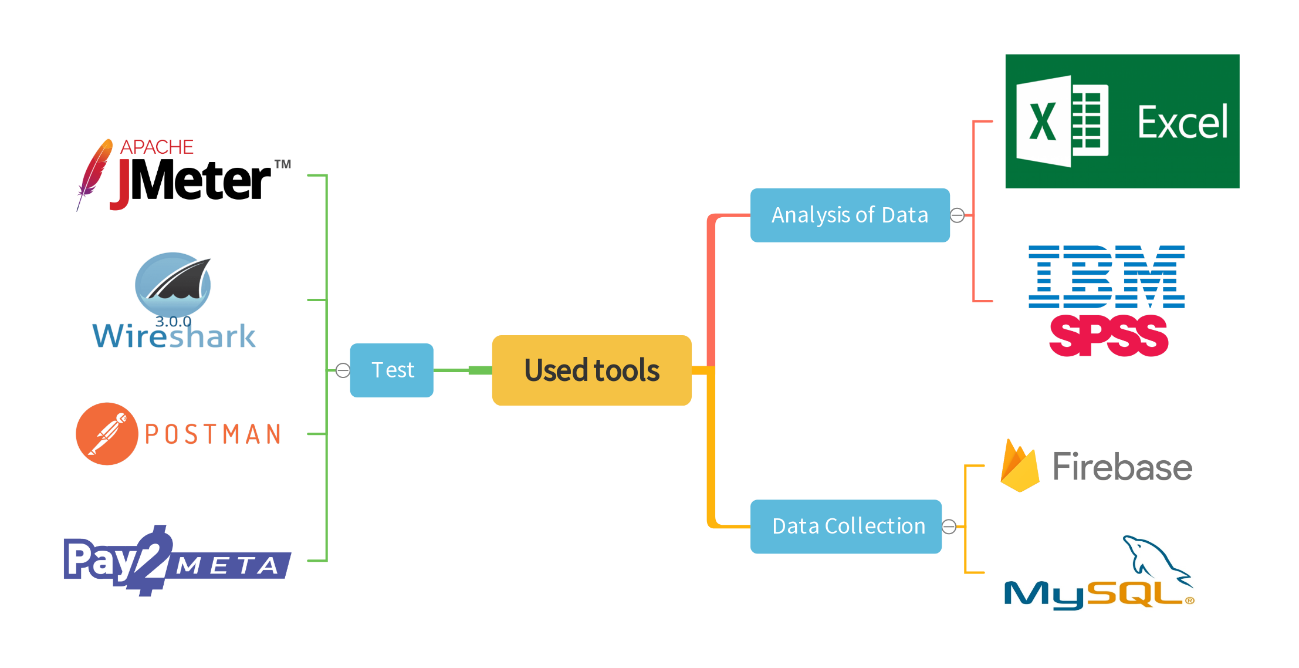


Figure : Used tools

**5.2 Pruebas de funcionamiento**

Para la protección de secretos digitales como llaves privadas, claves API, tokens entre otros se hará uso de la herramienta IOTA Stronghold, para esto se es necesario tener instalado en el equipo el lenguaje de programación Rust y posteriormente el paquete “cargo” que se encargará de ejecutar las librerías necesarias para el funcionamiento de Stronghold, el comando para su instalación es el siguiente:

**Instalación de cargo*:*** *cargo install --path .*

Una vez instalado el paquete cargo, el siguiente paso es instalar la herramienta stronghold utilizando el siguiente comando “cargo run –stronghold”, posteriormente se procede a realizar el almacenamiento de las claves privadas hacia la base de datos criptográfica de IOTA Stronghold. A continuación, se detalla el comando para realizarlo, se puede utilizar un texto plano con todas las claves a encriptar o directamente escribir un arreglo de claves.

**Comando utilizado*:*** *stronghold encrypt --plain privateKey.txt --record\_path “/home/fernando\_castillo/apps/proyecto” --pass Fernando\_1994.-*

La aplicación de IOTA se ve reflejado en la figura 30 donde se almacenó el pago de una transacción realizada en la aplicación Pay2Meta, el resultado se puede observar en el siguiente link que proviene de la Mainnet de IOTA:

<https://explorer.iota.org/mainnet/message/08aba58ca3bbf5879cbe9368cc02e7ad9f1d392abf4c70495f1aaae277632b8b>

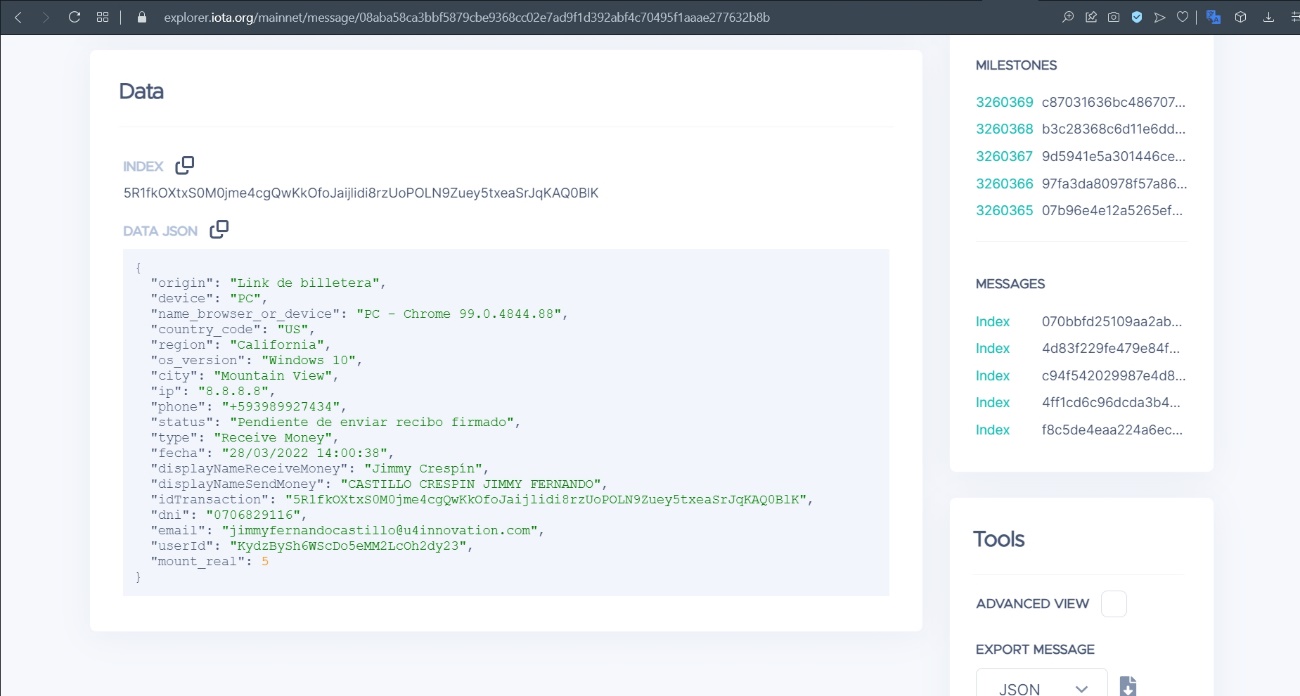


Figure : Transactional storage with IOTA

Con respecto a las encriptaciones, los DLT encriptan la información que circulan por la red WLAN pero no encriptan la información que proviene por la red LAN, por tal motivo se utilizó la librería de nodejs llamada jsencrypt para realizar encriptaciones de tipo RSA desde las aplicaciones clientes, para esto fue necesario que cada usuario tenga sus propias claves públicas y privadas. A continuación, se muestra el comando de como generar una llave privada de 4096 bit utilizando Openssl.

*openssl genrsa -out rsa\_4096\_priv.pem 4096*

A continuación, se muestra el comando de como generar una llave pública de 4096 bit utilizando Openssl.

*openssl rsa -pubout -in rsa\_4096\_priv.pem -out rsa\_4096\_pub.pem*

Finalmente, un ejemplo de encriptación desde el cliente se ve ilustrado en la figura 31 donde se utiliza la librería JSEncrypt conjuntamente con la llave pública generada para el usuario, se encripta con RSA información de la transacción como ip, datos del usuario e información financiera de la tarjeta de crédito. Esta información posteriormente será desencriptada por el servidor utilizando la llave privada del usuario almacenada en IOTA Stronghold.

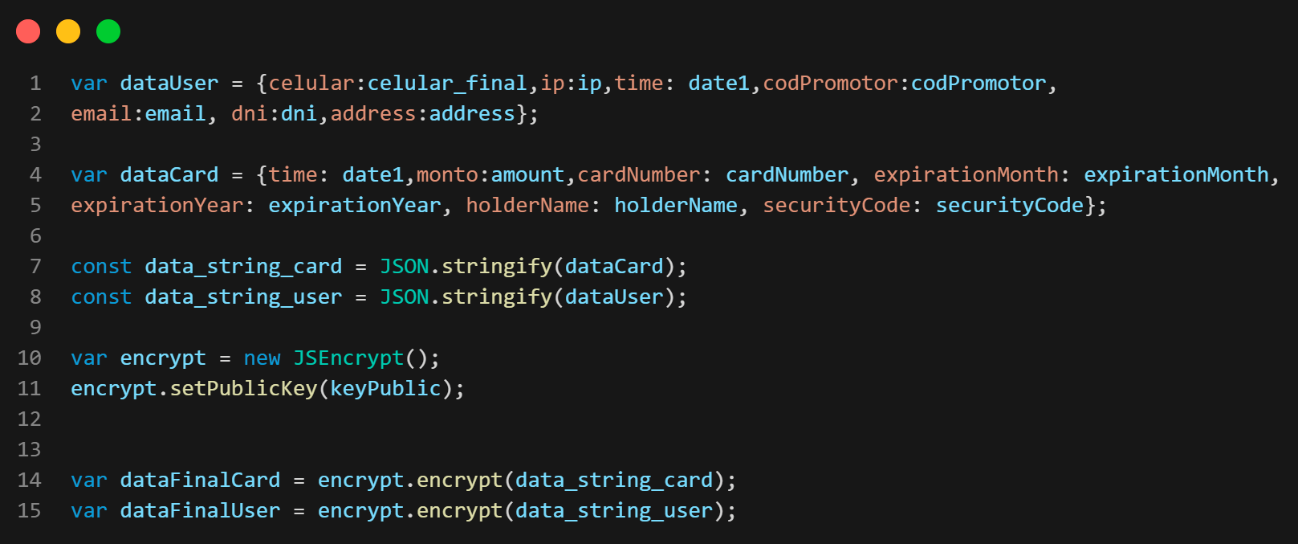


Figure : RSA encryption process

La aplicación y ejecución de los smart contracts ERC-20 se realizan al finalizar los procesos de compra/venta del Marketplace de criptomonedas que ofrece la plataforma Fintech Pay2Meta y para esto consta de los siguientes pasos:

1. Realización de compra/venta de criptomonedas en Pay2Meta.

En la figura 32 se ilustra el proceso de compra de criptomonedas donde los usuarios previamente ya se encuentran verificados biométricamente y con identidad digital.



Figure : Buying cryptocurrencies on Pay2Meta

1. Compilación del código solidity en Iotex Studio web IDE.

Una vez realizado una compra o venta en los Marketplace se procede a la compilación del código del smart contract ERC-20 ilustrado anteriormente en la figura 26, este proceso de compilar el smart contract se lo puede realizar utilizando el IDE web que ofrece Iotex (https://ide.iotex.io/), esto da como resultado un bytecode y un código ABI que será necesario posteriormente para deployar el smart contract.

1. Desplegar el smart contract con Iotex.

Una vez que se obtenga el código de bytes del paso anterior, el siguiente paso es deployar el smart contract enviándolo a la red de cadena de bloques de IoTeX. En la figura 33 se ilustra el código en nodeJS para deployar un smart contract con Iotex, el código otorga un hash que sería el address del contrato que se utilizará en el último paso.



Figure : Source code to implement a smart contract with Iotex

1. Ejecutar la transferencia del token ERC-20 con Tatum.

El último paso es realizar la transferencia del pago en criptomonedas al comercio, esto se realiza una vez que se haya completado todo el proceso del marketplace, para esto se ejecutará el endpoint ofrecido por la plataforma blockchain de Tatum donde se establece sobre que cadena de blockchain se hará la transferencia, en este caso ETH, también se define a cual address se enviará, la cantidad en criptomonedas, el address del contrato generado anteriormente y finalmente la llave privada del dueño de la billetera de Ethereum, a continuación se presenta el endpoint de tipo POST que se utilizó para la transferencia de criptomonedas conjuntamente con los parámetros de envio.

**Post:** <https://api-eu1.tatum.io/v3/blockchain/token/transaction>

{

"chain": "ETH",

"to": " 0x10a21aa67e615ddd1e63aa8d106c684279453ff5",

"amount": "0.0096222",

"contractAddress": "0x45871ED5F15203C0ce791eFE5f4B5044833aE10e",

"fromPrivateKey": "mi\_llave\_privada\_de\_mi\_billetera"

}

El resultado de ejecutar el endpoint se ve reflejado en el siguiente link donde se encuentra la transacción del pago realizado en la ropsten de pruebas de Ethereum:

<https://ropsten.etherscan.io/tx/0x04c72bf9f80ab620750f17313839cf4da2b670304d9a145a6388d26a4c2b3b83>

Para la aplicación de la identidad digital con NFT, primeramente, los usuarios deben realizar una verificación biométrica utilizando la plataforma Mati (<https://www.es.getmati.com>), donde se les solicita a los usuarios subir una foto de la parte frontal y trasera del documento de identidad y finalizar con la grabación de un video de unos tres segundos del rostro del usuario. En la figura 34 se ilustra el paso final de esta verificación biométrica.



Figure : Biometric Verification with MATI

Una vez finalizado la verificación biométrica, hay que esperar un tiempo en el que el sistema MATI a través de inteligencia artificial valide los documentos enviados por los usuarios. El resultado de la verificación biométrica es un documento pdf que se lo puede observar en el siguiente link:

https://firebasestorage.googleapis.com/v0/b/backservicespagos.appspot.com/o/verificacionBiometrica.pdf?alt=media&token=bf4baf87-32f7-40cf-a2a8-75ce3ddd3249

Finalmente, con la información verificada del usuario se genera un código QR con su identidad verificada biométricamente. El código QR generado, ilustrado en la figura 35, redireccionada a un registro de IOTA para asegurar la inmutabilidad de la verificación del usuario.



Figure : Code QR Biometric Verification

El siguiente paso es convertir la imagen del QR en una identidad digital con NFT. Al igual que en los smart contract ERC-20, el código utilizado para los NFT hay que compilarlo y deployarlo con Iotex y obtener el código ABI y el bytecode para posteriormente obtener el address del contrato. Con ese address del contrato se procede a utilizar el endpoint de Tatum para acuñar un nuevo token ERC-721, un ejemplo del endpoint junto con los parámetros utilizados son los siguientes:

**Post:** <https://api-eu1.tatum.io/v3/nft/mint>

{

"chain": "ETH",

"to": "0x10a21aa67e615ddd1e63aa8d106c684279453ff5",

"contractAddress": "0x1860Cf5A199892BC527A0698e7be08a7C6Bc064",

"url": " https://pay2meta.com/public/nft\_100.json",

"authorAddresses": [

"0x4eec1a0a2ae9bb1d9601101d429005b10da994f3"

],

"fromPrivateKey": "mi\_llave\_privada",

}

De manera opcional, el usuario puede publicar su NFT en la plataforma Opensea, un ejemplo de esto se lo puede observar en el siguiente link:

<https://opensea.io/assets/0x495f947276749ce646f68ac8c248420045cb7b5e/7523418735891926846006348340043757648305025013495208722884814318985145221121/>

**5.3 Pruebas de seguridad**

La seguridad de los datos se encuentra garantizados dentro del Tangle o Blockchain debido al uso de sus protocolos de consenso y a los diferentes algoritmos de encriptación que utilizan cada uno de ellos, pero ningún DLT garantiza la seguridad de los datos enviadas desde las aplicaciones clientes hacia los DLT por tal motivo es importante realizar un correcto análisis del tráfico de la red para prevenir ataques del tipo hombre en el medio y así evitar la escucha y desciframiento de los datos enviados para su posterior almacenamiento en los DLT. Para testear la seguridad del envío de datos desde aplicaciones clientes, se utilizó una de las funcionalidades ofrecidas por la plataforma Pay2Meta llamada links de billetera, en la figura 36 se ilustra el pago exitoso de cinco dólares realizados con una tarjeta de crédito VISA en uno de los links de billeteras de Pay2Meta.

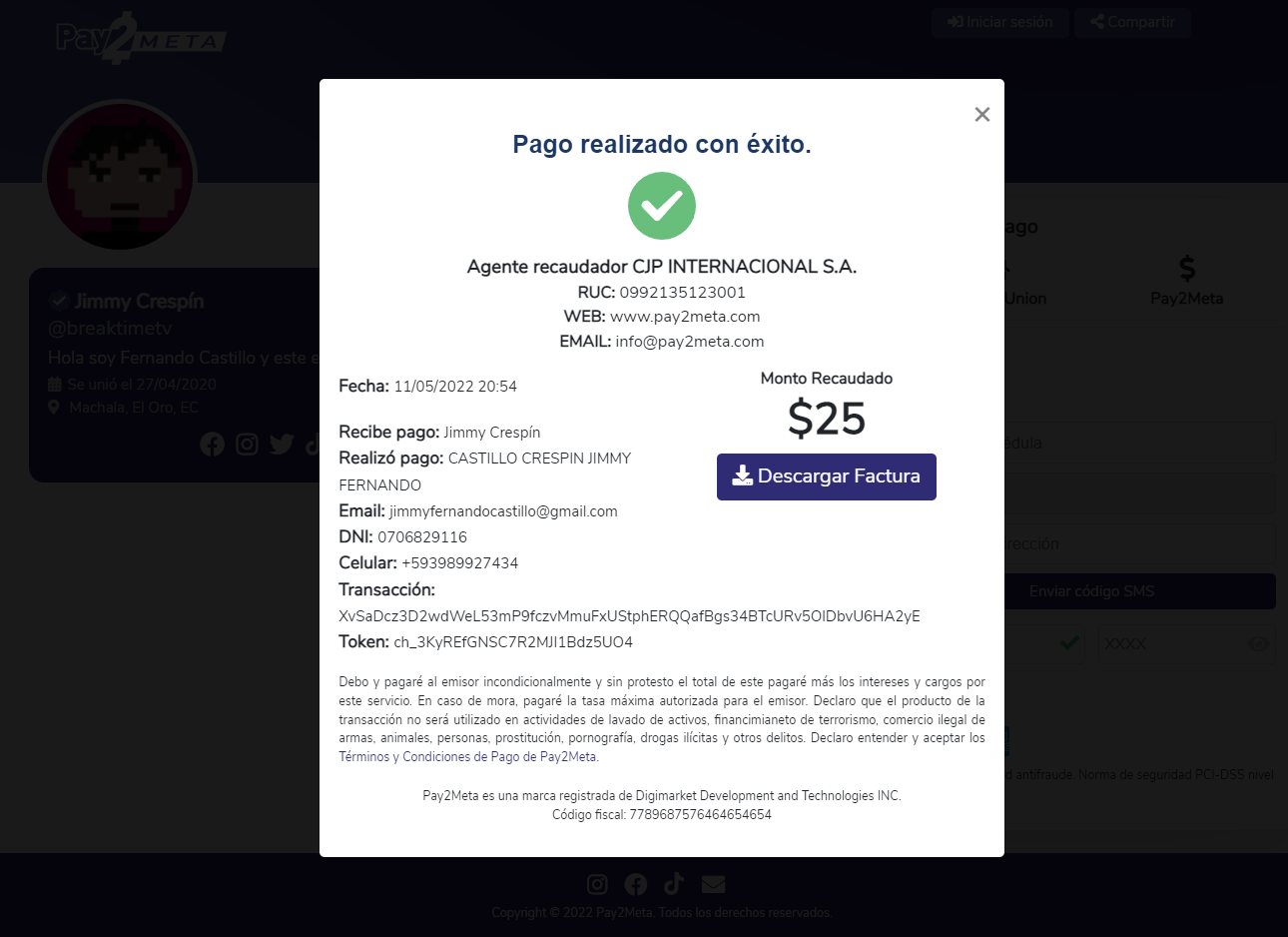


Figure 36: Confirmation of payment with Visa credit card

Los datos enviados a través del formulario de pago fueron encriptados con RSA, en la figura 37 se ilustra los datos obtenidos al momento de realizar la petición Post, en este caso los datos de la tarjeta con la que se realizó el pago y los datos personales del cliente, ambos parámetros fueron encriptados con RSA.

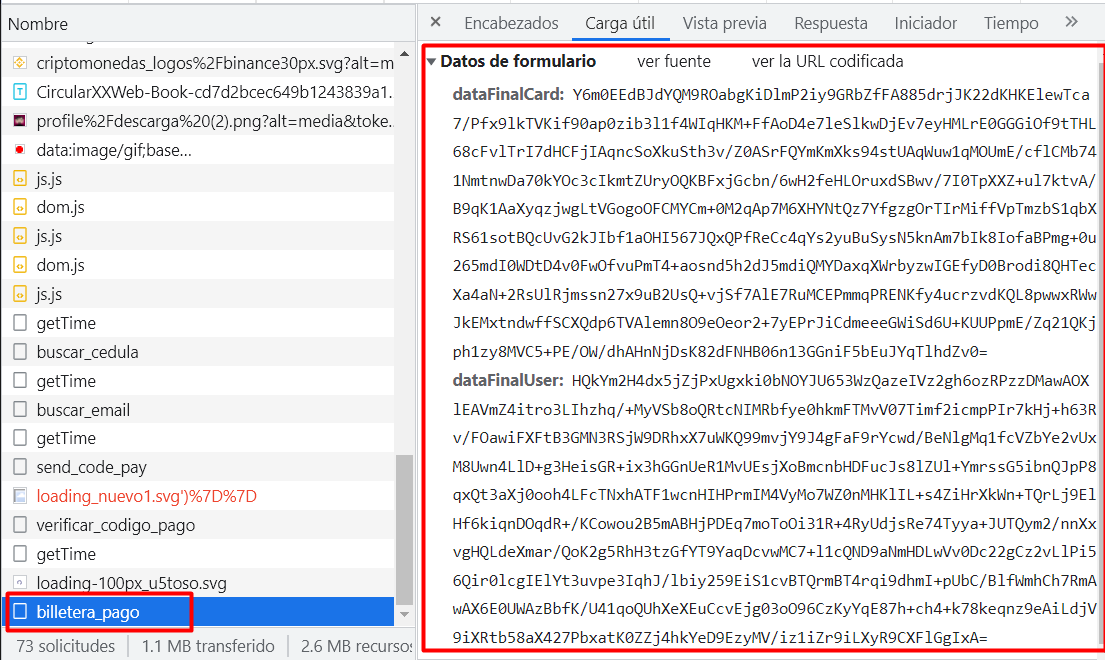


Figure 37: RSA encryption in payments made with credit cards

Esta encriptación se validó utilizando la herramienta wireshark, en la figura 38 se ilustra el tráfico http de tipo post donde se visualiza que los datos enviados del pago realizado anteriormente están encriptados.

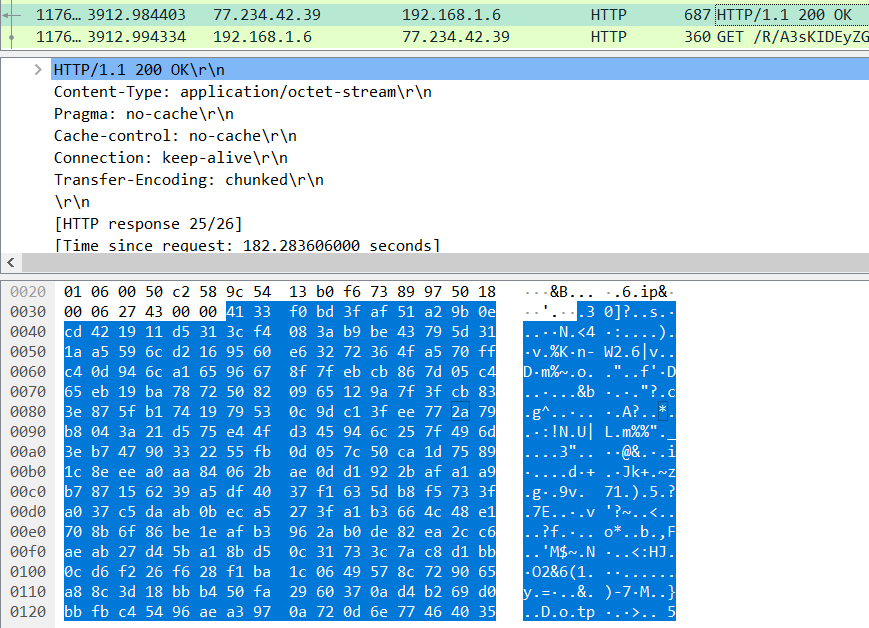


Figure 38: Network traffic in wireshark

**5.4 Pruebas de rendimiento**

Con los equipos mencionados en el experimento setup se realizaron pruebas de envíos de datos transaccionales a través de Postman, en la figura 49 se ilustra como a través de un endpoint de tipo Post se consiguió simular pagos transaccionales al mismo tiempo con una cantidad de 1000 usuarios obtenidos de la base de datos Firebase y con el card\_id de una tarjeta de crédito de pruebas. Esto se logró dividiendo procesos a través de microservicios y eventos proporcionados por Google Cloud Platform realizando pagos asincrónicamente, es decir en paralelo y al mismo tiempo como se ilustra en la figura 40 de los resultados en la consola de Firebase functions del endpoint utilizado.



Figure 39: Sending transactions with Postman

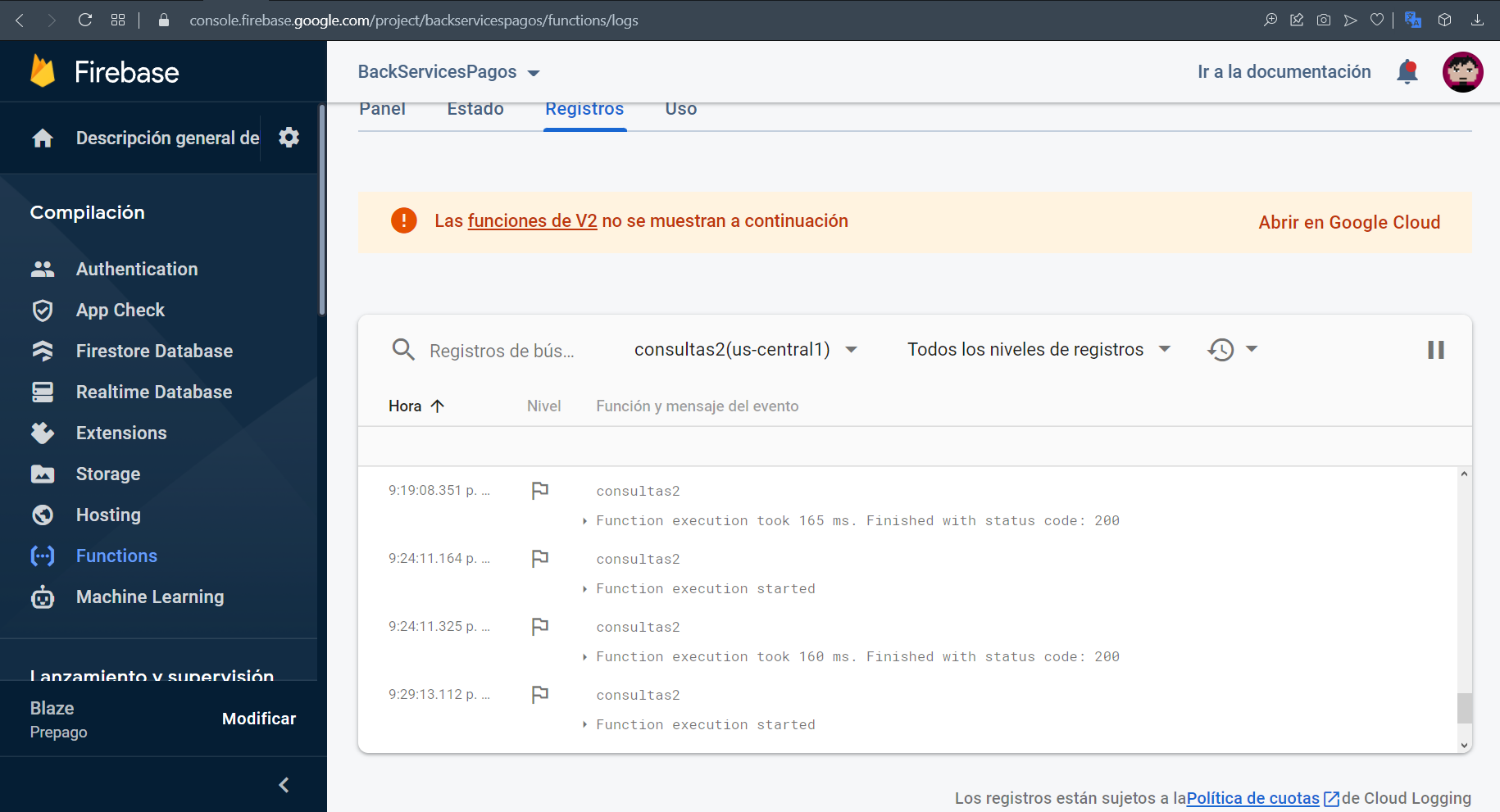


Figure 40: Firebase functions console of running transactions

**5.5 Pruebas de latencia**

La captura de información se lo realizó con JMeter y se determinó que existe una alta transaccionalidad debido a que se ejecutaron exitosamente todos los microservicios de Google Cloud con DLT, en la figura 41 se ilustra la secuencia realizada en el proceso de una transacción financiera, el mismo que está conformado por varios nodos que corresponden a los microservicios ejecutados, iniciando con el microservicio del pago (1) con un tiempo de 1s, seguido del almacenamiento en IOTA (2) con un tiempo de 20.5 s, ejecución del smart contract (3) con un tiempo de 3.5s y finalmente el microservicio de notificación (4), tomando un total de 25 segundos por transacción.

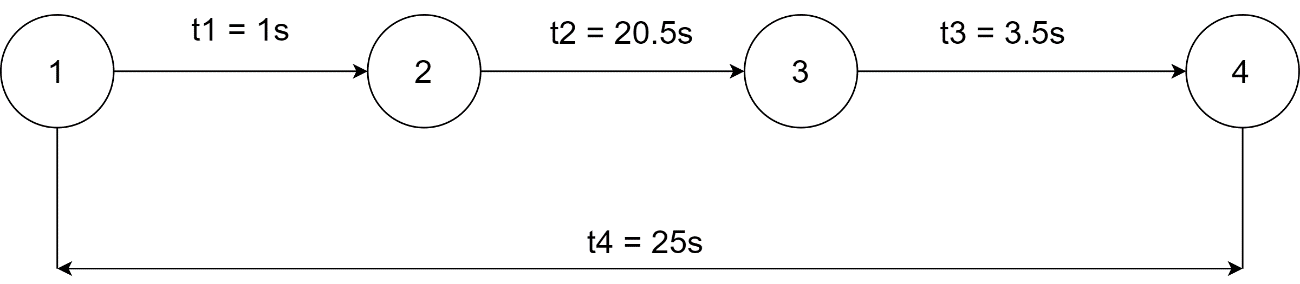


Figure 41: Performance measurement times

**5.6 Aplicación del coeficiente de correlación de Spearman**

Para determinar el tipo de correlación y verificar la hipótesis planteada en esta investigación se utilizó el coeficiente de Spearman debido a que los datos a trabajar eran de tipo no paramétricas. En la tabla 5 se ilustra la asignación de rangos de los datos de los DLT ejecutados y fraudes o estafas ganados y está conformada primeramente por la columna semanas que representan las 14 semanas que duró la investigación.

Con respecto a la columna de DLT ejecutados, estas cantidades fueron obtenidos de un registro histórico en Firebase de la plataforma Pay2Meta, provenientes de la ejecución de los smart contracts ERC-20 cuando se realizaron las compras/ventas de los marketplaces en conjunto con los registros transaccionales con IOTA y NFT.

En la columna de fraudes y estafas ganadas, estas cantidades se obtuvieron por disputas ganadas con la plataforma de pagos Stripe, en casos de fraudes con tarjetas de crédito/débito y por disputas ganadas con los usuarios de tipo comercio de la plataforma Pay2Meta en casos de estafas.

La columna Rango A está formada por la cantidad de registros analizados (14 registros) asignando el número mayor al valor mayor de la columna de DLT ejecutados y así sucesivamente hasta llegar al valor menor que sería uno. Un ejemplo práctico sería el registro #3 que posee un valor de 44 en la columna DLT ejecutados, que se le asignó el número 14 en la columna de Rango A, seguido del registro #2 con valor 25 en la columna DLT ejecutados asignándole el número 13 en la columna Rango A y así sucesivamente.

Con respecto a la columna de Rango B, sigue la misma secuencia realizada para la columna de Rango A, solamente que en vez de tomar los valores de la columna DLT ejecutados, se toma los valores de la columna de fraudes y estafas ganados. La columna “d” es la resta entre los rangos A y B y finalmente la columna “d^2” corresponde a la potencia dos de la columna “d”.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **#** | **Weeks** | **Executed DLT** | **Earned Scams** | **Rank A** | **Rank B** | **d** | **d^2** |
| 1 | 1 | 20 | 32 | 11 | 14 | -3 | 9 |
| 2 | 2 | 25 | 23 | 13 | 8 | 5 | 25 |
| 3 | 3 | 44 | 54 | 14 | 13 | 1 | 1 |
| 4 | 4 | 18 | 12 | 9 | 9 | 0 | 0 |
| 5 | 5 | 7 | 5 | 3 | 2 | 1 | 1 |
| 6 | 6 | 5 | 2 | 2 | 1 | 1 | 1 |
| 7 | 7 | 9 | 11 | 4 | 10 | -6 | 36 |
| 8 | 8 | 12 | 8 | 6 | 3 | 3 | 9 |
| 9 | 9 | 2 | 4 | 1 | 4 | -3 | 9 |
| 10 | 10 | 19 | 14 | 10 | 5 | 5 | 25 |
| 11 | 11 | 16 | 18 | 8 | 7 | 1 | 1 |
| 12 | 12 | 23 | 21 | 12 | 12 | 0 | 0 |
| 13 | 13 | 14 | 16 | 7 | 11 | -4 | 16 |
| 14 | 14 | 11 | 15 | 5 | 6 | -1 | 1 |
|  |  |  |  |  |  | **Sum** | 134 |

Tabla 5: Assignment of data ranges

Una vez finalizado con la tabla de valores, se aplica la fórmula de Spearman ilustrado en la figura 42, donde:

Rs= coeficiente de spearman

D= la suma total obtenido de d^2

n= cantidad de sujetos que se clasifican



Figure : Spearman's coefficient formula

Entonces:

Rs=

Para corroborar el resultado obtenido anteriormente se utilizó el software SPSS. En la tabla 6 se ilustra el resultado obtenido para Rho de 0,895.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Correlations | | | | |
|  | | | Executed\_DLT | Earned\_scams |
| Spearman’s Rho | Executed\_DLT | Correlation coefficient | 1,000 | ,895\*\* |
| Sig. (bilateral) | . | ,000 |
| N | 14 | 14 |
| Earned\_scams | Correlation coefficient | ,895\*\* | 1,000 |
| Sig. (bilateral) | ,000 | . |
| N | 14 | 14 |
| \*\*. The correlation is significant at the level 0,01 (bilateral). | | | | |

Tabla 6: Spearman Correlation in SPSS

Debido a que el valor calculado manualmente del rs es igual a 0.70 y en SPSS fue de 0.89 se concluye que existe una correlación positiva significativa. Por tanto, mientras más se implementen los DLT en procesos financieros, también aumentarán la cantidad de disputas ganadas por fraudes o estafas de primera persona en pagos realizados en aplicaciones Fintech.

Análisis de resultados

A continuación, se analizan los resultados obtenidos con trabajos previos de otros autores, entre los cuales se destacan los siguientes:

* + 1. Seguridad contra ataques man-in-the- middle.

A pesar de que la seguridad que brindan los DLT es alta, esta solamente abastece la encriptación de la información dentro de los nodos de los DLT pero la seguridad dentro de la red local entre aplicaciones cliente y la utilización de secretos digitales (llaves privadas, contraseñas, tokens, etc) en los microservicios aún queda expuesta a ataques de tipo man in the middle. En especial en aplicaciones Fintech donde existe un constante flujo de información tipo sensible, por tal motivo, esta investigación aporta con la utilización de una encriptación RSA con tamaño de 4096 bits en sus llaves públicas y privadas para brindar protección a los datos que provengan de las aplicaciones clientes hacia los microservicios. Además, dentro de los microservicios se empleó una conexión con la base de datos criptográfica de IOTA Stronghold para obtener, cuando se requiera, los secretos digitales necesarios para el funcionamiento de los endpoints.

Este aporte mejoraría con el trabajo realizado por Ekparinya [148] donde midió el impacto de los ataques man-in-the-middle sobre la red blockchain de Ethereum, pero en sus pruebas realizadas no contempló la utilización de algún algoritmo de encriptación para la conexión con la red, lo que supondría una vulnerabilidad de filtración de las llaves privadas de las billeteras Ethereum utilizadas en dicho experimento. También contribuiría en el trabajo realizado por Riadi [153] donde utilizaron una encriptación de tipo SHA256 en las aplicaciones clientes, pero dentro de sus microservicios para la conexión con base de datos no existe protección, creando una posible vulnerabilidad, caso contrario a esta investigación donde se utilizó IOTA Stronghold para mitigar este problema.

* + 1. Identidad digital con NFT.

Aunque actualmente existen varios algoritmos de machine learning para detectar fraudes que realizan las personas con tarjetas de créditos en sus pagos online como se observa en el trabajo realizado por Dornadula [162], el problema de fraudes aún persiste. Por tal motivo, aunque la plataforma Pay2Meta utiliza su propio sistema machine learning antifraude, en esta investigación añade una capa de seguridad adicional al utilizar un algoritmo de verificación biométrica a los usuarios para posteriormente convertirla en un NFT. Obteniendo así una identidad digital dentro del blockchain, aumentando así las probabilidades de reducir los casos de fraudes con apoyo de los algoritmos de machine learning estudiados en el trabajo de Dornadula.

* + 1. Transacciones con comisiones cero con IOTA.

Una de las preocupaciones más comunes que poseen los usuarios al utilizar aplicaciones financieras son los costos que estas cobrarán por las transacciones que se realicen. En especial aquellas transacciones que involucren criptomonedas. Sin embargo, el aporte ofrecido en esta investigación al no cobrarse comisiones por la utilización de IOTA cuando se almacenan transacciones financieras en su Tangle, que gracias a su inmutabilidad servirán de apoyo durante el dispute de fraudes de primera persona con las entidades bancarias, los usuarios no perderán su dinero y se brinda un nivel de confianza adicional a la plataforma Fintech, por los pagos realizados de los usuarios. Muchas aplicaciones Fintech utilizan blockchain para el almacenamiento de información, donde los usuarios asumen el pago de comisiones, un ejemplo de esto se observa en el trabajo realizado por Karaivanov [115], que utiliza la red Ethereum pagando comisiones altas, con nuestra solución utilizando IOTA no se añaden estos costos al usuario.

* + 1. Comisiones bajas de smart contracts con Iotex.

En nuestra investigación preliminar se obtuvo que Iotex cobra una comisión relativamente más baja que otras blockchain al momento de ejecutar un smart contract, comparado con Zarir [125] que utiliza la red Ethereum para ejecutar los smart contracts, con costos de comisión entre los 3$ a 10$ en criptomonedas, nuestra propuesta con Iotex presenta una comisión mucho más baja, de solo 0.35 centavos a 2$ en criptomonedas.

* + 1. Aplicación de la metodología ABCDE.

Las aplicaciones de tipo marketplace con pagos online actuales típicamente utilizan metodologías de desarrollo que no incluyen a los DLT en sus ciclos de vida, un ejemplo de ello aparece en Seitz & otros [172]. En nuestro trabajo se aporta a la comunidad científica, con la propuesta de uso de metodologías ABCDE para este tipo de aplicaciones, resolviendo así la problemática planteada.

El desarrollo de este proyecto abre paso a la investigación de varios trabajos futuros que por cuestiones de tiempo, alcance y falta de madurez de algunas tecnologías no se lograron implementar, entre estas se destacan los contratos inteligentes y NFT con IOTA debido a que se encuentran en fase beta, lo que imposibilita su implementación en un ambiente de producción, situación similar ocurre con el DLT Radix Tempo que por su falta de madurez no se contempló su utilización en esta investigación y finalmente la blockchain 4.0 que involucra la inteligencia artificial, debido a que el alcance de esta investigación se estableció solo para la blockchain 2.0 y 3.0.

CONCLUSIONES

La investigación concluyó exitosamente con todos los objetivos planteados comprobando la hipótesis de que si se implementa tecnologías de registros distribuidos (DLT) en una arquitectura de microservicios cloud se incrementa la probabilidad de ganar disputas financieras por casos de estafas y fraudes de primera persona en transacciones financieras online de sistemas DApps fintech.

El uso de los DLT incrementa la seguridad en transacciones financieras online debido a los protocolos de consenso que utilizan, esto sumado a la seguridad ofrecida por Google Cloud en sus microservicios y a las encriptaciones RSA o AES aplicadas en las aplicaciones clientes, todos estos aspectos ayudaron a mitigar casos de estafas y fraudes de primera persona en conjunto con la utilización de smarts contracts e identidad digital con NFT.

La selección de los DLT depende exclusivamente de la naturaleza del proyecto a realizarse por tal motivo es necesario la realización de un SLR para conocer las ventajas y desventajas que estas proveen y elegir las que más se ajusten a las características del proyecto.

La aplicación de la metodología ABCDE resultó ser eficaz para el desarrollo de los sistemas Dapp en la arquitectura de microservicios de Google Cloud utilizada en esta investigación, incluyendo el uso del DLT en sus ciclos de vida.

Con los aportes realizados en nuestro trabajo, se logró construir una Fintech segura, rápida, con tiempos de almacenamiento de apenas 20.5 s en la cloud, costos de comisiones cero o muy bajos, alta confiabilidad y respaldo a los usuarios, gracias a la inmutabilidad de las transacciones.

Quedó demostrado la aceptación de los usuarios por obtener una identidad digital con verificación biométrica y NFT con un resultado del 98% de aceptación y esto sumado a la utilización de códigos PIN, huella dactilar o código de Google Authenticator que ayudaron a la mitigación de fraudes de primera persona al momento de realizar pagos online, ya que todos estos aspectos serían pruebas irrefutables de una persona realizando compras por internet en una aplicación Fintech.

Se obtuvo mayor rentabilidad económica para la plataforma Fintech con un total de ganancias por disputas ganadas de $2.566,39 frente a los $559,36 por las disputas perdidas en el tiempo de pruebas de tres meses. También los usuarios de la plataforma Fintech obtuvieron rentabilidad económica al momento de utilizar smart contract por las bajas comisiones ofrecidas por Iotex blockchain en comparación con otras tecnologías como Ethereum o Bitcoin.

RECOMENDACIONES

Para trabajar con smart contract o NFT es necesario contar con al menos una billetera de criptomoneda por cuestión de pago de comisiones y cada billetera maneja sus propias claves privadas, que al ser robadas puede provocar el robo del dinero en estas billeteras, por tal motivo se recomienda el uso de IOTA Stronghold para salvaguardar estas llaves privadas y no almacenarlas dentro de archivos del propio proyecto o dentro de base de datos no criptográficas.

Los smart contract están expuestos a vulnerabilidades, por tal motivo se recomienda el uso de alguna herramienta de análisis de seguridad del código generado para los smart contract, en esta investigación se hizo uso de Mythril que resultó ser eficaz para detectar vulnerabilidades antes de proceder con el deploy del mismo.

Las tecnologías de registros distribuidos aseguran seguridad de encriptación en redes WAN pero no en redes LAN, por tal motivo se recomienda la utilización de algoritmos de encriptación como AES o RSA para mitigar estas vulnerabilidades presentes en las aplicaciones clientes.

# 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]. [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]. [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, 2020. |
| [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] | 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. |
| [25] | 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. |
| [26] | 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. |
| [27] | 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. |
| [28] | J. Novillo-Vicuña, D. H. Rojas, B. M. Olivo, J. M. Ríos y O. C. Villavicencio, «Arduino y el internet de las cosas,» 3Ciencias, 2018. |
| [29] | J. Novillo, D. Hernández, B. Mazón, J. Molina y O. Cárdenas, «Arduino y el Internet de las cosas,» *Área de Innovación y Desarrollo, SL, España,* 2018. |
| [30] | 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. |
| [31] | F. Guo, X. Xiao, A. Hecker y S. Dustdar, «Characterizing IOTA Tangle with Empirical Data,» *IEEE Global Communications Conference,* pp. 1-6, 2020. |
| [32] | D. Hernandez-Rojas, B. Mazón-Olivo y C. Escudero, «Internet de las cosas (IoT),» *Análisis de Datos Agropecuarios,* vol. 1, pp. 71-100, 2018. |
| [33] | 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. |
| [34] | D. Hernández-Rojas, «Sistema de Telemetría basado en redes WSN (Wireless Sensor Network) para el Internet de las Cosas (IoT),» 2018. |
| [35] | D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas y C. J. Escudero, «Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through BLE beacons in IoT telemetry applications,» *Sensors,* vol. 18, nº 1, p. 57, 2017. |
| [36] | D. Hernandez-Rojas, B. Mazon-Olivo, J. Novillo-Vicuña, C. Escudero-Cascon, A. Pan-Bermudez y G. Belduma-Vacacela, «IoT android gateway for monitoring and control a WSN,» *International Conference on Technology Trends, Springer,* pp. 18-32, 2017. |
| [37] | I. Foundation, «IOTA Smart Contracts Beta Release,» 2021. [En línea]. [Último acceso: 21 10 2021]. |
| [38] | 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. |
| [39] | 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. |
| [40] | 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. |
| [41] | 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. |
| [42] | B. Mazon-Olivo, D. Hernández-Rojas, J. Maza-Salinas y A. Pan, «Rules engine and complex event processor in the context of internet of things for precision agriculture,» *Computers and Electronics in Agriculture,* vol. 154, pp. 347-360, 2018. |
| [43] | K. Hausken, «Cyber resilience in firms, organizations and societies,» *Internet of Things,* vol. 11, 2020. |
| [44] | 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. |
| [45] | L. Abdillah, «An Overview of Indonesian Fintech Application,» *The First International Conference on Communication, Information Technology and Youth Study (I-CITYS2019),* 2019. |
| [46] | 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. |
| [47] | 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. |
| [48] | 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. |
| [49] | 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. |
| [50] | S. Nick, «Formalizing and Securing Relationships on Public Networks,» *First Monday,* 1997. |
| [51] | M. Rahouti, K. Xiong y N. Ghani, «Bitcoin Concepts, Threats, and Machine-Learning Security Solutions,» *IEEE Access,* vol. 6, pp. 67189-67205, 2018. |
| [52] | C. C. Vergara y L. F. Agudo, «Fintech and Sustainability: Do They Affect Each Other?,» *Sustainability,* vol. 13, nº 13, p. 7012, 2021. |
| [53] | M. Xu, X. Chen y G. Kou, «A systematic review of blockchain,» *Financial Innovation,* vol. 5, nº 27, 2019. |
| [54] | 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. |
| [55] | 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,. |
| [56] | 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. |
| [57] | 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. |
| [58] | 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. |
| [59] | 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. |
| [60] | 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. |
| [61] | 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. |
| [62] | 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. |
| [63] | 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. |
| [64] | A. d. Vries y C. Stoll, «Bitcoin's growing e-waste problem,» *Resources, Conservation and Recycling,* vol. 175, 2021. |
| [65] | 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. |
| [66] | 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. |
| [67] | A. d. Vries, «Renewable Energy Will Not Solve Bitcoin’s Sustainability Problem,» *Joule,,* vol. 3, nº 4, pp. 893-898, 2019. |
| [68] | 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. |
| [69] | D. F. Maesa, «Blockchain 3.0 applications survey,» *Journal of Parallel and Distributed Computing,* vol. 138, pp. 99-114, 2020. |
| [70] | 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. |
| [71] | 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. |
| [72] | 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. |
| [73] | 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. |
| [74] | 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. |
| [75] | 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. |
| [76] | 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. |
| [77] | 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. |
| [78] | 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. |
| [79] | 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. |
| [80] | 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. |
| [81] | 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. |
| [82] | 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. |
| [83] | J. Angelis y E. R. d. Silva, «Blockchain adoption: A value driver perspective,» *Business Horizons,* vol. 62, nº 3, pp. 307-314, 2019. |
| [84] | 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. |
| [85] | U. Bodkhe, «Blockchain for Industry 4.0: A Comprehensive Review,» *IEEE Access,* vol. 8, pp. 79764-79800, 2020. |
| [86] | A. M. Campoverde, D. L. Hernández y B. E. Mazón, «Cloud computing con herramientas open-source para Internet de las cosas,» *Maskana,* vol. 6, pp. 173-182, 2015. |
| [87] | 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. |
| [88] | A. Hannousse y S. Yahiouche, «Securing microservices and microservice architectures: A systematic mapping study,» *Computer Science Review,* vol. 41, 2021. |
| [89] | N. Mateus-Coelho, M. Cruz-Cunha y L. G. Ferreira, «Security in Microservices Architectures,» *Procedia Computer Science,* vol. 181, pp. 1225-1236, 2021. |
| [90] | 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. |
| [91] | 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. |
| [92] | 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. |
| [93] | 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. |
| [94] | 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. |
| [95] | G. S. Sadasiuvam, «A critical review on using blockchain technology in education domain,» *Handbook of Deep Learning in Biomedical Engineering,* pp. 85-121, 2021. |
| [96] | N. O. Nawari y Shriraam Ravindran, «Blockchain and the built environment: Potentials and limitations,» *Journal of Building Engineering,* vol. 25, 2019. |
| [97] | B. Farahani, F. Firouzi y M. Luecking, «The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions,» *Journal of Network and Computer Applications,* vol. 177, 2021. |
| [98] | A. I. Sanka y R. C. Cheung, «A systematic review of blockchain scalability: Issues, solutions, analysis and future research,» *Journal of Network and Computer Applications,* vol. 195, 2021. |
| [99] | X. Fu, H. Wang y P. Shi, «A survey of Blockchain consensus algorithms: mechanism, design and applications,» *Science China Information Sciences,* vol. 64, 2021. |
| [100] | Y. Lu, «The blockchain: State-of-the-art and research challenges,» *Journal of Industrial Information Integration,* pp. 80-90, 2019. |
| [101] | 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. |
| [102] | A. Donmez y A. Karaivanov, «Transaction fee economics in the Ethereum blockchain,» *Economic Inpuiry,* vol. 60, nº 1, pp. 265-292, 2021. |
| [103] | H. -N. Dai, Z. Zheng y Y. Zhang, «Blockchain for Internet of Things: A Survey,» *IEEE Internet of Things Journal,* vol. 6, nº 5, pp. 8076-8094, 2019. |
| [104] | G. Sargsyan, N. Castellon, R. Binnendijk y P. Cozijnsen, «Blockchain Security by Design Framework for Trust and Adoption in IoT Environment,» *2019 IEEE World Congress on Services (SERVICES),* pp. 15-20, 2019. |
| [105] | R. Yang, R. Wakefield, S. Lyu, S. Jayasuriya, F. Han, X. Yi, X. Yang, G. Amarasinghe y S. Chen, «Public and private blockchain in construction business process and information integration,» *Automation in Construction,* vol. 118, 2020. |
| [106] | A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi y A. S. A.-M. AL-Ghamdi, «Blockchain Platforms and Access Control Classification for IoT Systems,» *Symmetry,* vol. 12, nº 10, 2020. |
| [107] | D. C. Nguyen, P. N. Pathirana, M. Ding y A. Seneviratne, «Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges,» *IEEE Communications Surveys & Tutorials,* vol. 22, nº 4, pp. 2521-2549, 2020. |
| [108] | X. Fan y Q. Chai, «Roll-DPoS: A Randomized Delegated Proof of Stake Scheme for Scalable Blockchain-Based Internet of Things Systems,» *In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous '18),* 2018. |
| [109] | D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas y C. J. Escudero, «A plug-and-play human-centered virtual TEDS architecture for the web of things,» *Sensors,* vol. 18, nº 7, p. 2052, 2018. |
| [110] | 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. |
| [111] | Q. Wang, R. Li, Q. Wang y S. Chen, «Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges,» *Cryptography and Security,* 2021. |
| [112] | 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. |
| [113] | N. Khan, B. Kchouri, N. A. Yatoo, Z. Kräussl, A. Patel y R. State, «Tokenization of sukuk: Ethereum case study,» *Global Finance Journal,* 2020. |
| [114] | Tatum, «Welcome to Tatum,» 2021. [En línea]. [Último acceso: 02 11 2021]. |
| [115] | Tatum, «Supported Blockchains,» 2021. [En línea]. [Último acceso: 02 11 2021]. |
| [116] | 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. |
| [117] | 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. |
| [118] | 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. |
| [119] | S. Popov y W. Buchanan, «FPC-BI: Fast Probabilistic Consensus within Byzantine Infrastructures,» *arXiv,* 2021. |
| [120] | S. Popov, «IOTA: Feeless and Free,» *IEEE Blockchain Technical Briefs,* 2019. |
| [121] | A. Panarello, N. Tapas, G. Merlino, F. Longo y A. Puliafito, «Blockchain and IoT Integration: A Systematic Survey,» *Sensors,* vol. 18, nº 8, 2018. |
| [122] | I. Foundation, «The Coordicide,» 2019. [En línea]. |
| [123] | 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. |
| [124] | I. Foundation, «The new Chrysalis Network is Live!,» IOTA, 2021. [En línea]. [Último acceso: 2021]. |
| [125] | I. Team, «Introducing IOTA Stronghold,» 19 07 2020. [En línea]. [Último acceso: 20 01 2022]. |
| [126] | 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. |
| [127] | 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. |
| [128] | 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. |
| [129] | 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. |
| [130] | 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. |
| [131] | 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. |
| [132] | 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. |
| [133] | P. Ekparinya, V. Gramoli y G. Jourjon, «Impact of Man-In-The-Middle Attacks on Ethereum,» *IEEE 37th Symposium on Reliable Distributed Systems (SRDS),* pp. 11-20, 2018. |
| [134] | J. Cartuche, D. Hernández, R. Morocho y CiroGarcía, «Seguridad IoT: Principales amenazas en una taxonomía de activos,» *HAMUT'AY,* vol. 7, nº 3, pp. 51-59, 2021. |
| [135] | 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. |
| [136] | 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. |
| [137] | R. Kumar y R. Goyal, «On cloud security requirements, threats, vulnerabilities and countermeasures: A survey,» *Computer Science Review,* vol. 33, pp. 1-48, 2019. |
| [138] | I. Riadi, R. Umar, I. Busthomi y A. W. Muhammad, «Block-hash of blockchain framework against man-in-themiddle attacks,» *Jurnal Ilmiah Teknologi Sistem Informasi,* 2021. |
| [139] | 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. |
| [140] | 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. |
| [141] | P. Kumar y S. B. Rana, «Development of modified AES algorithm for data security,» *Optik,,* vol. 127, nº 4, pp. 2341-2345, 2016. |
| [142] | 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. |
| [143] | E. Huseynov y J.-M. Seigneur, «Chapter 50 - Context-Aware Multifactor Authentication Survey,» *Computer and Information Security Handbook (Third Edition),* pp. 715-726, 2017. |
| [144] | V. N. Dornadula y S. Geetha, «Credit Card Fraud Detection using Machine Learning Algorithms,» *Procedia Computer Science,* vol. 165, pp. 631-641, 2019. |
| [145] | 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. |