



## UNIVERSIDAD TECNOLÓGICA ISRAEL

### ESCUELA DE POSGRADOS “ESPOG”

### MAESTRÍA EN SEGURIDAD INFORMÁTICA

*Resolución:* RPC-SO-02-No.053-2021

#### PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

<b>Título del proyecto:</b>
Propuesta de aplicación de blockchain en transacciones de pasarelas de pago en Ecuador para mejorar su seguridad
<b>Línea de Investigación:</b>
Ciencias de la ingeniería aplicada a la producción, sociedad y desarrollo sustentable
<b>Campo amplio de conocimiento:</b>
Tecnologías de la información y la comunicación (TIC)
<b>Autora:</b>
Kerly Prisila Naranjo Paez
<b>Tutores:</b>
Mg. Renato Mauricio Toasa Guachi PhD Maryory Urdaneta Herrera

Quito – Ecuador

2024

## APROBACIÓN DEL TUTOR



Yo, **Renato Mauricio Toasa Guachi** con C.I: **1804724167** en mi calidad de Tutor del proyecto de investigación titulado: PROPUESTA DE APLICACIÓN DE BLOCKCHAIN EN TRANSACCIONES DE PASARELAS DE PAGO EN ECUADOR PARA MEJORAR SU SEGURIDAD.

Elaborado por: **Kerly Prisila Naranjo Paez**, de C.I: **1726773169**, estudiante de la Maestría en Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

---

**Firma**

**ORCID: 0000-0002-2138-300X**

## APROBACIÓN DEL TUTOR



Yo, **Maryory Urdaneta Herrera** con C.I: **1759316126** en mi calidad de Tutor del proyecto de investigación titulado: PROPUESTA DE APLICACIÓN DE BLOCKCHAIN EN TRANSACCIONES DE PASARELAS DE PAGO EN ECUADOR PARA MEJORAR SU SEGURIDAD.

Elaborado por: **Kerly Prisila Naranjo Paez**, de C.I: **1726773169**, estudiante de la Maestría en Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

---

**Firma**

**ORCID: 0000-0001-8773-5349**

## DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE



Yo, Kerly Prisila Naranjo Paez con C.I: 1726773169, autora del proyecto de titulación denominado: PROPUESTA DE APLICACIÓN DE BLOCKCHAIN EN TRANSACCIONES DE PASARELAS DE PAGO EN ECUADOR PARA MEJORAR SU SEGURIDAD. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autora del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2024

**Firma**

**ORCID:** 0009-0007-1489-9992

## Tabla de contenidos

APROBACIÓN DEL TUTOR	2
APROBACIÓN DEL TUTOR	3
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE	4
INFORMACIÓN GENERAL	1
Contextualización del tema	1
Problema de investigación	1
Objetivo general	2
Objetivos específicos	2
Vinculación con la sociedad y beneficiarios directos:	3
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO	4
1.1. Contextualización general del estado del arte	4
1.2. Proceso investigativo metodológico	6
1.3. Análisis de resultados	7
CAPÍTULO II: PROPUESTA	11
2.1 Fundamentos teóricos aplicados	11
2.2 Descripción de la propuesta	14
2.3 Valoración de la propuesta	25
2.4 Matriz de articulación de la propuesta	26
CONCLUSIONES	32
RECOMENDACIONES	33
BIBLIOGRAFÍA	34
ANEXOS	36

## Índice de tablas

Tabla 1. Matriz de articulación

26

## Índice de figuras

Figura 1. Interfaz de una pasarela de pago lista para el ingreso de datos y pago en línea .....	8
Figura 2. Registro de una transacción exitosa a través de una pasarela de pago .....	9
Figura 3. Funcionamiento de la tecnología blockchain .....	13
Figura 4. Funcionamiento de una pasarela de pago en línea.....	16
Figura 5. Propuesta diseñada para implementar blockchain.....	19

## **INFORMACIÓN GENERAL**

El presente proyecto de titulación establece una propuesta para la aplicación de la tecnología blockchain en transacciones de pasarelas de pago en Ecuador con el fin de mejorar la seguridad.

### **Contextualización del tema**

Tener transacciones seguras en pasarelas de pago es primordial para garantizar la confianza de los usuarios y proteger sus datos financieros. La tecnología blockchain puede desempeñar un papel importante en mejorar la seguridad y la transparencia en este ámbito. (Vidal, 2022)

La presente propuesta pretende disminuir vulnerabilidades en la seguridad de datos, reducir tiempos de ejecución y asegurar la confidencialidad, disponibilidad e integridad de los datos de transacciones en línea.

Para lograr cumplir con los objetivos se empieza con la identificación de vulnerabilidades y amenazas inherentes en las transacciones, se desarrollan registros de seguridad que ayudan a mitigar riesgos de seguridad. De la misma manera, se investiga los diferentes usos de los bloques de datos, lo cual permite desarrollar una propuesta, por medio de la obtención y recopilación de mejores prácticas, la cual se valora la comparar el flujo tradicional de una transacción con el flujo con tecnología blockchain.

Paralelo se estudian los flujos de las transacciones en diferentes proveedores, encontrando que éstas incluyen la aplicación de protocolos seguros enfocándose en la protección de los datos del usuario, independientemente del tipo de comercio. Es importante mencionar que los comercios electrónicos que manejan pasarelas de pago deben cumplir con la normativa vigente ecuatoriana para la protección de datos personales. (Batz, 2021)

### **Problema de investigación**

Actualmente las pasarelas de pago tienen ciertas limitaciones en términos de seguridad y eficiencia en comparación con las soluciones basadas en blockchain. Las pasarelas de pago suelen centralizar los datos de las transacciones en servidores controlados por la entidad que opera la pasarela. Esto puede ser un punto de vulnerabilidad, ya que, si estos servidores son comprometidos por atacantes, se corre el riesgo de que la información financiera y los datos personales de los usuarios sean robados. (Guarderas, 2022)

Entre otras soluciones convencionales, los detalles de las transacciones generalmente no están abiertos para su inspección por parte de los usuarios. Esto puede generar desconfianza y dificultar la verificación de las transacciones.

Las pasarelas de pago tradicionales pueden estar expuestas a ataques de fraude y cargos no autorizados. Los atacantes podrían explotar las vulnerabilidades en los sistemas de autenticación o interceptar los datos de tarjetas de crédito para realizar transacciones fraudulentas. (Vidal, 2022)

Es importante mencionar que la seguridad en las pasarelas de pago tradicionales se ha mejorado considerablemente a lo largo de los años y muchas empresas han implementado medidas de seguridad robustas para proteger las transacciones y los datos de los usuarios. Sin embargo, la tecnología blockchain tiene el potencial de revolucionar la seguridad y la eficiencia de las transacciones en las pasarelas de pago, además ofrece características como la descentralización, la inmutabilidad y la transparencia que pueden abordar algunos de los desafíos mencionados anteriormente en el contexto de las transacciones en línea. (Hernández, 2021)

¿Con una apropiada aplicación de blockchain, se puede mejorar la seguridad en las transacciones en pasarelas de pago en Ecuador?

### **Objetivo general**

Definir una propuesta de aplicación de blockchain aplicable al proceso de seguridad en transacciones de pasarelas de pago ecuatorianas.

### **Objetivos específicos**

- Contextualizar los fundamentos teóricos sobre seguridad y blockchain.
- Identificar las posibles vulnerabilidades y amenazas en el flujo de una transacción bancaria a través de una pasarela de pago.
- Diseñar una propuesta que contribuya a la aplicación de blockchain como técnica de seguridad en el proceso de transacciones de pago en línea.
- Valorar el diseño de la propuesta tomando en cuenta el criterio de especialistas en seguridad con amplia experiencia y conocimiento en seguridad de la información.

**Vinculación con la sociedad y beneficiarios directos:**

La implementación de blockchain en pasarelas de pago puede aportar varios beneficios significativos a la sociedad. Estos beneficios se derivan de las características únicas de la tecnología blockchain y su capacidad para mejorar la seguridad, la eficiencia y la transparencia en las transacciones financieras en línea. Los principales beneficiarios de la presente propuesta son los usuarios que realizan compras de bienes o servicios en internet y hacen uso de sus tarjetas bancarias para completar la orden y adquirir el bien.

En particular, la presente propuesta se enfoca en el Objetivo de Desarrollo Sostenible número nueve estrechamente relacionado a la innovación, la cual es considerada una clave para descubrir una solución duradera que brinde seguridad, eficiencia y confianza a las personas al momento de realizar una compra en línea. Además, estimula la innovación en el sector de los servicios financieros. Puede llevar al desarrollo de nuevas soluciones tecnológicas y modelos comerciales que aprovechen las características de seguridad y eficiencia de blockchain.

## CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

Para el presente proyecto se toma referencias de diferentes fuentes de investigación relacionadas a la seguridad y protección de información bancaria, así como documentos que detallen a profundidad conceptos fundamentales de blockchain y su aplicación en diferentes áreas.

### 1.1. Contextualización general del estado del arte

A continuación, se enlista los libros, artículos y documentos que conforman el estado del arte para la presente propuesta.

**Título:** Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World

**Autores:** Don Tapscott y Alex Tapscott, 2016

**Objetivo del aporte:** El libro explora el potencial disruptivo de blockchain en diferentes sectores, como las finanzas, la salud, la energía y más.

**Aporte a la presente investigación:** Los autores describen a blockchain como una tecnología que va mucho más allá de Bitcoin y las criptomonedas. Aunque Bitcoin fue la primera aplicación exitosa de blockchain, esta tecnología tiene una amplia gama de casos de uso en diversas industrias y campos. Basado en la opinión de los autores, esta afirmación da paso a profundizar el tema propuesto y descubrir el potencial de blockchain en pasarelas de pago. (Tapscott , 2016)

**Título:** The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology

**Autor:** William Mougayar, 2016

**Objetivo del aporte:** El autor examina cómo blockchain está transformando los modelos de negocio y ofrece una visión general de las aplicaciones prácticas de esta tecnología.

**Aporte a la presente investigación:** Se toma la propuesta del autor y se concluye que blockchain está teniendo un impacto significativo en la transformación de los modelos de negocio en diversas industrias. Su capacidad para proporcionar seguridad, transparencia, descentralización y eficiencia en las transacciones y registros permite reevaluar e imaginar como operarían los comercios y proveedores ecuatorianos. (Mougayar, 2016)

**Título:** Electricity Billing System using Ethereum and Firebase

**Autor:** Dim En Nyaung & May Hlaing. 2019

**Objetivo del aporte:** El escrito propone un sistema de facturación de electricidad basado en la tecnología blockchain de Ethereum y la plataforma de desarrollo de aplicaciones móviles Firebase de Google. El sistema busca mejorar la eficiencia y transparencia en el proceso de facturación eléctrica, aprovechando las características de seguridad y descentralización de Ethereum y la capacidad de desarrollo rápido de aplicaciones de Firebase. Se describe cómo el sistema utiliza contratos inteligentes en Ethereum para gestionar y registrar transacciones de consumo de electricidad de manera segura y transparente, y cómo se integra con Firebase para proporcionar una interfaz de usuario intuitiva y accesible para los usuarios finales. El documento detalla la arquitectura del sistema, los componentes clave y el proceso de implementación, destacando los beneficios potenciales de esta solución, como la reducción de fraudes y errores, la automatización de procesos y la mejora de la confianza entre proveedores de energía y consumidores.

**Aporte a la presente investigación:** Se toma del documento principalmente la flexibilidad que ofrece la tecnología blockchain en cuanto a su aplicación, ya que puede ser utilizada y ajustada en una amplia variedad de industrias, sin importar su naturaleza diversa. Según Hlaing y Nyaung, se están desarrollando soluciones que combinan blockchain con otras tecnologías, como contratos inteligentes, para mejorar aún más la eficiencia y seguridad de las transacciones. Estos contratos permiten automatizar procesos y garantizar el cumplimiento de acuerdos entre las partes involucradas. (Hlaing y Nyaung, 2019)

**Título:** Análisis de pertinencia de una solución de diseño de bloques de seguridad en transacciones descentralizadas para el gobierno electrónico ecuatoriano.

**Autores:** Recalde Varela Pablo Marcel, Ramos Rodríguez Andrés Ricardo. 2023

**Objetivo del aporte:** La tesina en mención propone una solución que aporta seguridad y transparencia a procesos gubernamentales.

**Aporte a la presente investigación:** Los autores describen una solución de diseño de cadena de bloques haciendo énfasis en las características únicas que ofrece blockchain, como la descentralización, la transparencia y la seguridad. El análisis de esta solución está estrechamente relacionado con el presente trabajo debido a la evaluación de las necesidades

de implementar blockchain para contribuir a la transformación digital del sector público en Ecuador. (Recalde y Ramos, 2023)

## **1.2. Proceso investigativo metodológico**

Se implementa una investigación bibliográfica, de análisis y por observación directa las cuales tienen como objetivo identificar y comprender las técnicas y estrategias utilizadas por las pasarelas de pago, así como desarrollar planes de acción para abordar los efectos de los ataques y prevenir futuros incidentes.

### **Investigación bibliográfica**

A la investigación bibliográfica se la puede definir como un proceso sistemático de búsqueda, recopilación, revisión y análisis de la literatura existente sobre un tema específico. Este tipo de investigación se basa en el examen de fuentes de información disponibles en forma de libros, revistas, artículos, tesis, informes, documentos electrónicos y otras publicaciones académicas y científicas. (Cortés, 2012)

El objetivo principal de la investigación bibliográfica es obtener una comprensión completa y actualizada del estado del conocimiento sobre el análisis de la presente propuesta. Al realizar la investigación bibliográfica, se identifica las teorías, enfoques metodológicos, hallazgos, debates y tendencias relevantes. Esto con el fin de contextualizar la investigación y comprender cómo la propuesta contribuye en las existentes pasarelas de pago ecuatorianas.

### **Investigación por observación directa**

La metodología de investigación por observación directa implica la recolección de datos observando directamente un fenómeno, evento o comportamiento en su entorno natural, sin manipulación por parte del investigador. Esta técnica se utiliza en una variedad de disciplinas para recopilar información detallada y contextualizada sobre el objeto de estudio. (Cortés, 2012)

Se busca crear una propuesta que facilite la adaptación e integración de la tecnología blockchain con el fin de mejorar la seguridad en las transacciones. Esta propuesta tiene como objetivo garantizar que las transacciones reflejen con precisión la información correspondiente a los consumos reales de los usuarios, además de mantener registros de datos inalterables en tiempo real sin necesidad de intermediarios. La metodología también pretende simplificar cada etapa del proceso, asegurando eficiencia, rentabilidad y una medición continua, al mismo tiempo que previene fraudes. Adicionalmente, busca proporcionar una visibilidad completa y transparente del proceso para todas las partes involucradas.

Esta propuesta se valida desde la investigación por observación directa realizada sobre el proceso de una transacción en línea, sus riesgos y amenazas y como estas pueden ser mitigadas con la aplicación de una cadena de bloques. Al aprovechar la descentralización y la inmutabilidad de la tecnología blockchain, se espera reducir los costos operativos, mitigar el riesgo de fraudes y agilizar el procesamiento de pagos. Además, al proporcionar un registro transparente y seguro de todas las transacciones, se fortalece la confianza tanto de los comerciantes como de los usuarios finales. Esta propuesta no solo busca modernizar las pasarelas de pago, sino también sentar las bases para un ecosistema financiero más sólido y confiable.

### **1.3. Análisis de resultados**

De acuerdo con la investigación y metodología descrita anteriormente se define como factible la propuesta de implementar tecnología blockchain en pasarelas de pago en Ecuador al igual que en cualquier otro país.

El análisis realizado mediante el método de observación directa implica la observación detallada de los procesos involucrados en las transacciones de pago en línea para identificar posibles puntos débiles y riesgos de seguridad. Las vulnerabilidades y amenazas detectadas mediante este método se describen a continuación.

**Fugas de datos sensibles:** Al observar los procesos de entrada de datos en las pasarelas de pago se pudo revelar posibles vulnerabilidades en la protección de información sensible, como direcciones y datos personales. La exposición inadvertida de estos datos puede resultar en robo de identidad o fraudes financieros.

**Ataques de intermediarios:** La comunicación entre el usuario, la pasarela de pago y el proveedor de servicios de pago puede revelar posibles puntos de vulnerabilidad donde los atacantes podrían intervenir y manipular la información durante la transmisión. Esto podría llevar a ataques de intermediarios, como la interceptación de datos o la suplantación de identidad.

**Vulnerabilidades en la autenticación:** Al observar el proceso de autenticación de usuarios se puede evidenciar buenos mecanismos de autenticación, sin embargo, con blockchain se puede implementar la utilización de identidades digitales descentralizadas almacenadas en la cadena de bloques, lo que garantiza la integridad y la inmutabilidad de la información de autenticación.

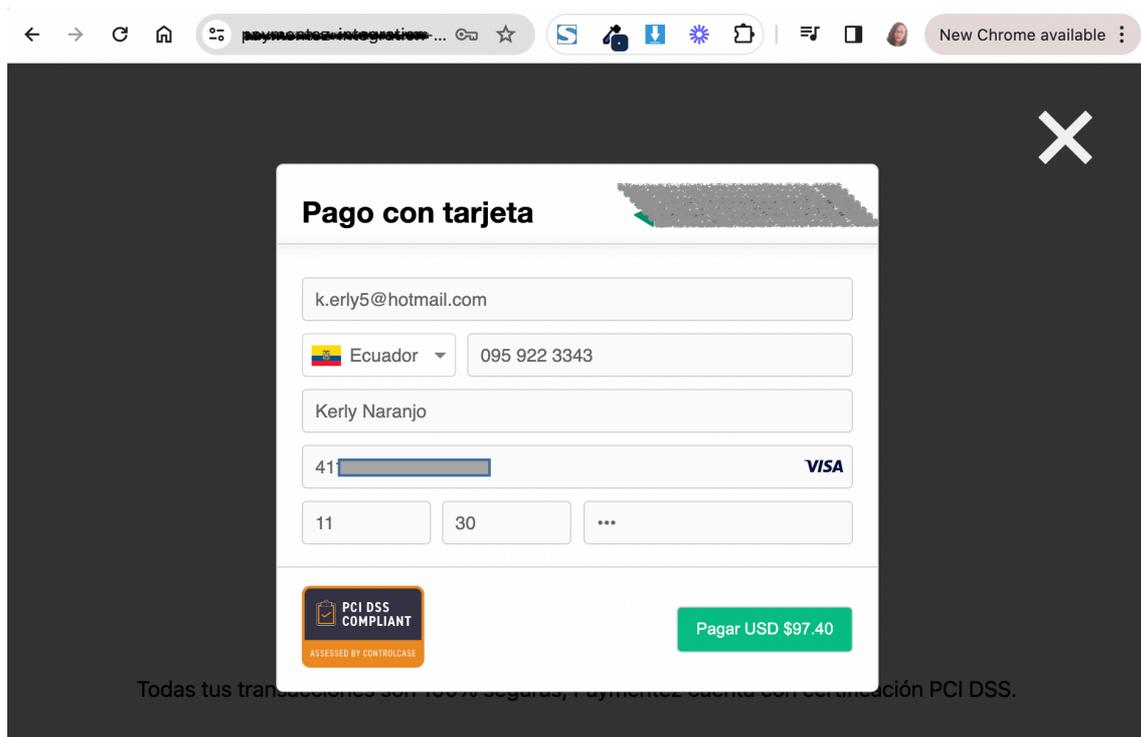
**Fallas en la seguridad del software:** Al observar la interacción del usuario con la interfaz de la pasarela de pago se determina que pueden existir vulnerabilidades en el software subyacente, como fallos de seguridad, inyecciones de código malicioso o debilidades en la gestión de sesiones.

**Ataques de Ingeniería Social:** Observar las interacciones entre el usuario y la pasarela de pago nos revela posibles tácticas de ingeniería social utilizadas por los atacantes para engañar a los usuarios y obtener información confidencial, como credenciales de inicio de sesión o detalles de tarjetas de crédito.

La *Figura 1* y la *Figura 2* muestran el paso de información sensible en un flujo de pago en línea.

**Figura 1.**

*Interfaz de una pasarela de pago lista para el ingreso de datos y pago en línea*



**Figura 2.**

*Registro de una transacción exitosa a través de una pasarela de pago*

```
card: {
  number: '████████████████████████████████████████',
  bin: '411111',
  type: 'vi',
  transaction_reference: 'DF-522547',
  status: '',
  token: '',
  expiry_year: '2030',
  expiry_month: '11',
  origin: 'Paymentez'
}
}
[utils/order.js] Transaction marked as paid, shopifyTransactionObj {"transaction": {"id": "6744106139821", "order_id": "4849975328941", "kind": "sale", "gateway": "Tarjeta de crédito o débito", "status": "success", "message": null, "created_at": "2024-03-11T12:49:25-05:00", "test": true, "authorization": "DF-522547###iEEtrp", "location_id": null, "user_id": null, "parent_id": "6048341262509", "processed_at": "2024-03-11T12:49:25-05:00", "device_id": null, "error_code": null, "source_name": "6943675", "receipt": {}, "amount": "97.40", "currency": "USD", "payment_id": "#1041.2", "total_unsettled_set": {"presentment_money": {"amount": "0.0", "currency": "USD"}, "shop_money": {"amount": "0.0", "currency": "USD"}}, "manual_payment_gateway": true, "admin_graphql_api_id": "gid://shopify/OrderTransaction/6744106139821"}

```

Este análisis permite tomar medidas proactivas para mitigar los riesgos y mejorar la seguridad del sistema. La propuesta de aplicación de blockchain ofrece varias herramientas y técnicas que pueden utilizarse para mejorar la autenticación y mitigar las vulnerabilidades en este proceso crítico de seguridad. Al implementar medidas como la autenticación basada en blockchain, la autenticación multifactorial y la gestión descentralizada de identidades, es posible crear un sistema de autenticación más robusto y resistente a ataques.

Existen también otros factores que deben ser considerados antes de llevar a cabo una implementación exitosa, uno de ellos es la regulación y cumplimiento, es importante comprender las regulaciones y requisitos legales en Ecuador con respecto a las criptomonedas, blockchain y las transacciones financieras en línea. Es importante trabajar en colaboración con las autoridades financieras para garantizar que la implementación cumpla con todas las leyes y regulaciones aplicables.

La implementación de blockchain requerirá una infraestructura tecnológica adecuada. Esto incluye la selección de la plataforma blockchain, el diseño y desarrollo de contratos inteligentes, la elección de protocolos de seguridad y otros aspectos técnicos. También es necesario considerar la interoperabilidad con sistemas y pasarelas de pago existentes, además requerirá la colaboración de diversas partes interesadas, incluyendo bancos, procesadores de

pagos, comerciantes, reguladores y posiblemente el gobierno. La cooperación es esencial para garantizar una adopción y ejecución efectivas. (Batz, 2021)

Otro aspecto muy importante para considerar al momento de implementar esta tecnología es la seguridad y privacidad, aunque blockchain es conocida por su seguridad, no está exenta de riesgos. Es importante implementar medidas de seguridad adecuadas para proteger los datos y las transacciones de los usuarios. También se debe considerar cómo se manejará la privacidad de los datos personales en la cadena de bloques.

Si bien blockchain ofrece seguridad y transparencia, algunas implementaciones pueden ser lentas y requerir una escalabilidad adecuada para manejar un alto volumen de transacciones en tiempo real. Adicionalmente los costos iniciales pueden ser significativos en términos de desarrollo, integración y capacitación.

En conclusión, se considera factible la idea de implementar tecnología de cadena de bloques en pasarelas de pago en Ecuador, pero se requiere una planificación cuidadosa, colaboración entre partes interesadas y cumplimiento de regulaciones locales. Si se abordan adecuadamente estos desafíos, la implementación de blockchain podría mejorar la seguridad y la eficiencia de las transacciones en las pasarelas de pago en el país.

## **CAPÍTULO II: PROPUESTA**

El presente trabajo presenta una propuesta de aplicación de blockchain en transacciones de pasarelas de pago ecuatorianas, a continuación, se definen los principales términos relacionados:

### **2.1 Fundamentos teóricos aplicados**

#### **Pasarela de pago**

Una pasarela de pago es una infraestructura tecnológica que permite la transferencia segura de información financiera entre un comercio en línea y el banco adquirente o procesador de pagos. En otras palabras, es el sistema que facilita y asegura la comunicación entre el cliente que realiza una compra en línea y la institución financiera que procesa la transacción.

Las pasarelas de pago son herramientas esenciales en el comercio electrónico. Su principal función es facilitar la autorización y la liquidación de transacciones electrónicas, como compras en línea, donaciones y otros tipos de transacciones financieras. (Tamayo, 2021)

#### **Transacción electrónica**

Una transacción electrónica es un intercambio de información, valor o servicios entre dos o más partes a través de medios electrónicos o digitales en lugar de realizarlo de manera física o presencial. Estas transacciones pueden abarcar una amplia gama de actividades, como compras en línea, transferencias de dinero, pagos de facturas, reservas de servicios, entre otros.

Las transacciones electrónicas involucran la transferencia de datos a través de redes de comunicación electrónica, como Internet u otras redes informáticas. Los datos que se intercambian pueden incluir información financiera, datos personales, productos digitales o servicios. (Lozano, 2015)

#### **Ley Orgánica de Protección de Datos Personales del Ecuador**

La Ley de Protección de Datos Personales de Ecuador es una normativa legal que tiene como objetivo proteger los derechos y la privacidad de las personas en relación con el tratamiento de sus datos personales. Esta ley establece los principios, derechos y obligaciones que deben cumplir tanto las entidades públicas como las entidades privadas al manejar información personal.

La ley se aplica a todas las personas naturales o jurídicas que realicen el tratamiento de datos personales en Ecuador. Los principios fundamentales para el tratamiento de datos

personales son el consentimiento informado, la finalidad legítima, la calidad y veracidad de los datos, la seguridad y confidencialidad, entre otros. Las entidades que tratan datos personales deben cumplir con ciertas obligaciones, como obtener el consentimiento del titular antes del tratamiento, implementar medidas de seguridad adecuadas para proteger los datos, notificar a los titulares sobre cualquier incidente de seguridad, entre otras.

La Agencia de Regulación y Control de Datos Personales (ARCO) es la entidad encargada de supervisar y regular el cumplimiento de la ley. Esta agencia tiene la facultad de recibir denuncias, realizar investigaciones y aplicar sanciones en caso de incumplimiento.

## **Blockchain**

Según Mougayar (2016) Blockchain es una tecnología de registro distribuido que permite el almacenamiento y la transferencia segura de información de manera descentralizada y transparente. Se basa en una cadena de bloques enlazados de forma cronológica y segura. Cada bloque contiene un conjunto de transacciones y un hash (firma digital) del bloque anterior, lo que crea una cadena inmutable y resistente a la manipulación. En la Figura 3 se puede observar el funcionamiento de blockchain. Las características clave incluyen:

**Descentralización:** La información se almacena en múltiples nodos de una red descentralizada. Esto reduce el riesgo de fallos únicos y aumenta la seguridad de la red.

**Transparencia:** Cada transacción registrada en la cadena de bloques es visible para todos los participantes de la red.

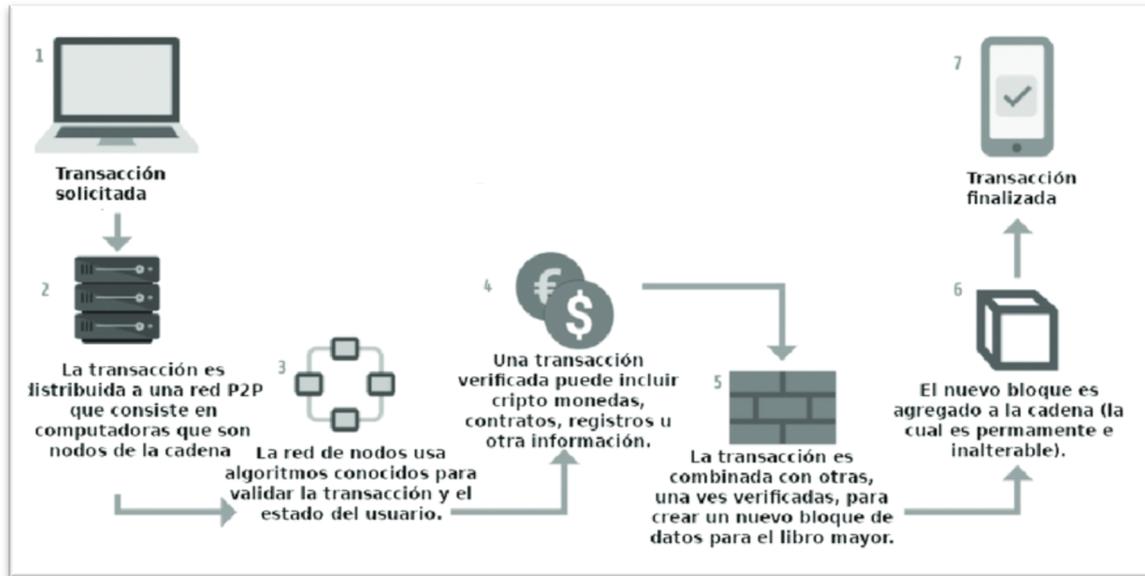
**Inmutabilidad:** Una vez que se registra una transacción en un bloque y se agrega a la cadena, no se puede modificar sin alterar todos los bloques siguientes, lo que hace que sea extremadamente difícil alterar el historial de transacciones.

**Seguridad criptográfica:** Las transacciones son aseguradas y verificadas a través de algoritmos de cifrado robustos.

**Contratos inteligentes:** Son programas autónomos que se ejecutan automáticamente cuando se cumplen ciertas condiciones predefinidas.

Blockchain se hizo ampliamente conocido como la tecnología subyacente de las criptomonedas como Bitcoin y Ethereum, pero su aplicabilidad se ha extendido mucho más allá del ámbito de las criptomonedas. Se ha explorado en diversas industrias como finanzas, cadena de suministro, atención médica, energía, votación electrónica, entre otros, debido a su capacidad para proporcionar confianza y seguridad en transacciones y registros. (Luna, 2022)

**Figura 3.**  
*Funcionamiento de la tecnología blockchain*



Nota: Obtenido de Fuentes et al. (2022)

### Vulnerabilidades

Las vulnerabilidades son fallos o debilidades en sistemas, aplicaciones, dispositivos o procesos que pueden ser explotados por amenazas o atacantes para comprometer la seguridad de dichos sistemas. Estas debilidades pueden permitir que los atacantes accedan, manipulen o dañen la información o los activos protegidos por esos sistemas. En términos simples, una vulnerabilidad es como una puerta abierta o una brecha en la defensa que los atacantes pueden aprovechar para ingresar o causar daño. (Luna, 2022)

### Amenazas en transacciones de pasarelas de pago

Según Guarderas (2022), las transacciones realizadas a través de pasarelas de pago en línea están expuestas a varias amenazas potenciales que podrían comprometer la seguridad y la integridad de los datos financieros y personales de los usuarios. Entre las amenazas más comunes se encuentran las siguientes.

**Riesgos de privacidad y robo de datos:** Los atacantes pueden intentar interceptar los datos de los usuarios, como información de tarjetas de crédito, contraseñas y otra información personal, mientras se transmiten entre el cliente y la pasarela de pago.

**Phishing:** Los atacantes pueden intentar engañar a los usuarios para que revelen sus datos confidenciales, como contraseñas y números de tarjeta de crédito, a través de correos electrónicos falsos o sitios web fraudulentos que imitan a pasarelas de pago legítimas.

**Man in the middle:** Los atacantes pueden intentar comprometer la seguridad de la pasarela de pago entre el cliente y el comerciante. Esto puede suceder cuando el atacante se sitúa entre el cliente y la pasarela para interceptar o modificar la información.

**Fraude con tarjetas de crédito:** Los atacantes pueden utilizar tarjetas de crédito robadas o falsificadas para realizar compras fraudulentas a través de pasarelas de pago. También pueden aprovechar vulnerabilidades en los sistemas de autenticación y validación.

**Ataques de inyección:** Los atacantes pueden intentar inyectar código malicioso o comandos en las solicitudes de pago para explotar vulnerabilidades en el sistema y obtener acceso no autorizado o manipular datos.

**Ataques de fuerza bruta:** Los atacantes pueden intentar adivinar contraseñas o números de tarjeta de crédito mediante el uso de programas automatizados que prueban una amplia gama de combinaciones.

**Denegación de servicio:** Los sistemas de la pasarela de pago podrían ser blanco de ataques de denegación de servicio (DDoS) u otros intentos de interrupción, lo que podría afectar la disponibilidad y el funcionamiento de las transacciones.

## 2.2 Descripción de la propuesta

En base a la investigación entre los proveedores de pasarelas de pago que operan en el país, se tiene que, actualmente el funcionamiento de una pasarela de pago implica varios pasos para facilitar una transacción en línea segura entre un comprador y un vendedor. El proceso generalizado se detalla a continuación:

**Inicio de una transacción:** Una vez que el cliente va a realizar una compra en línea, escoge los productos o servicios que desea adquirir y continua a la pantalla de pago.

**Elección de la pasarela de pago:** El cliente escoge el método de pago que prefiere utilizar, como tarjeta de crédito, tarjeta de débito u otros métodos de pago aceptados por el comercio.

**Redirección a la pasarela de pago:** Una vez que el cliente selecciona el método de pago, el sitio web o la aplicación lo redirige a la pantalla de la pasarela de pago. En este punto, el cliente digita su información para completar la transacción.

**Procesamiento de la información:** La pasarela de pago procesa la información proporcionada por el cliente y verifica si los datos son correctos y válidos.

**Autorización:** Una vez que se verifica la información la pasarela de pago se comunica con el banco emisor de la tarjeta para solicitar la autorización de la transacción y verificar si el cliente tiene suficientes fondos para realizar la compra.

**Aprobación o rechazo:** El banco emisor o el proveedor de la billetera digital responde a la solicitud de autorización de la pasarela de pago, indicando si la transacción es aprobada o rechazada.

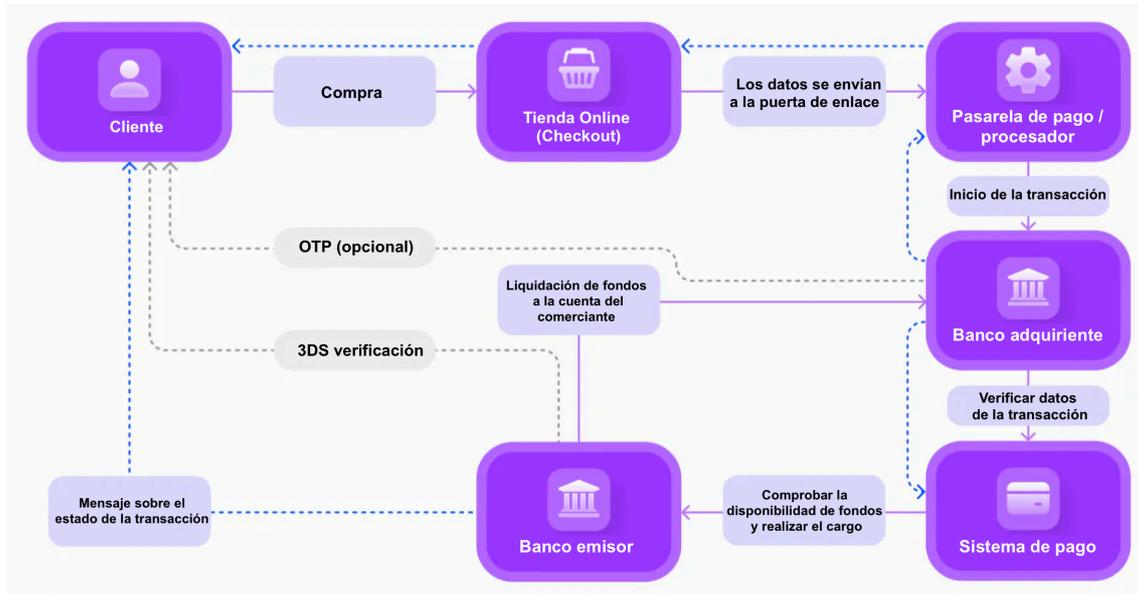
**Confirmación de la transacción:** La pasarela de pago envía un mensaje de confirmación al sitio web o la aplicación del comerciante, indicando si la transacción fue exitosa. En caso de éxito, se muestra al cliente una confirmación de la compra.

**Registro de la transacción:** La pasarela de pago registra la transacción en su sistema, generando un recibo electrónico que incluye detalles como el monto, la fecha, el comerciante y la información de la transacción.

**Liquidación y depósito:** La pasarela de pago inicia el proceso de liquidación, que implica transferir los fondos desde la cuenta del cliente al comercio. Dependiendo de la pasarela de pago y el acuerdo comercial, esto puede ocurrir de manera inmediata o en un horario predeterminado.

La Figura 4 muestra el funcionamiento actual de una pasarela de pago.

**Figura 4.**  
*Funcionamiento de una pasarela de pago en línea*



Nota: Elaborado a partir de Vidal (2022)

Parte esencial para el desarrollo de la propuesta es entender como encaja una cadena de bloques en el proceso actual de una transacción. La *Figura 5.* muestra el flujo de una pasarela con blockchain.

El funcionamiento de una pasarela de pago con blockchain implica varios pasos que combinan la tecnología blockchain con los procesos de pago tradicionales. Los componentes generales son:

**Inicio de la transacción:** El proceso comienza cuando un cliente realiza una compra en línea y elige pagar utilizando una pasarela de pago.

**Generación de la transacción:** Una vez que el usuario selecciona la opción de pago, se genera una transacción en la cadena de bloques que contiene la información relevante sobre la compra, como el monto, el vendedor y el comprador.

**Firma digital:** El comprador firma digitalmente la transacción utilizando su clave privada, lo que garantiza la autenticidad y la integridad de la transacción.

**Validación de la transacción:** La transacción se transmite a la red blockchain, donde es validada por los nodos de la red utilizando algoritmos de consenso. Los nodos verifican la validez de la transacción y su cumplimiento con las reglas predefinidas de la cadena de bloques.



**Figura 6.**  
*Blockchain como procesador de pago*



Nota: Elaboración propia basado en Blockchains (2022)

El funcionamiento de una pasarela de pago con seguridad blockchain implica la generación, firma, validación, inclusión y confirmación de transacciones en la cadena de bloques, proporcionando un método seguro, transparente y eficiente para procesar pagos en línea.

#### **a. Estructura general**

Una pasarela de pago desempeña un papel esencial en el proceso de compra en línea, asegurando que la información financiera se transmita de manera segura, que las transacciones sean autorizadas y que los fondos sean transferidos de manera adecuada entre las partes involucradas.

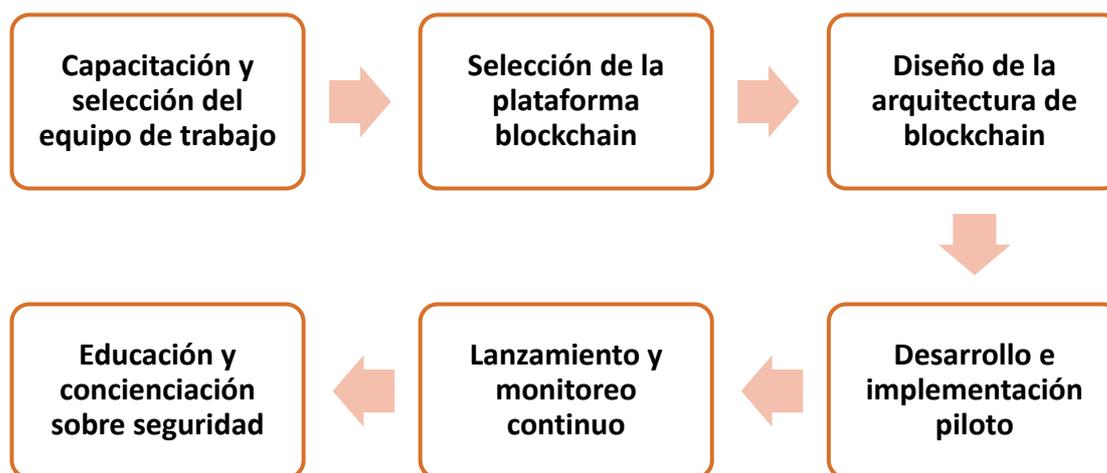
A continuación, se detalla la propuesta para la adaptación y aplicación de blockchain con el propósito de asegurar el proceso de transacciones de los comercios electrónicos, apuntando a los fundamentos de seguridad de datos utilizando la tecnología blockchain. “Cada evento o modificación de los datos se escriben como un nuevo bloque de una cadena y de esta

manera queda un registro asentado, certificado y se garantiza su integridad y disponibilidad”. Además, si el contenido se encuentra cifrado, garantiza confiabilidad. (Blockchains, 2022)

La Figura 7 muestra las etapas que conforman la presente propuesta que permitirán cumplir con el objetivo.

**Figura 7.**

*Propuesta diseñada para implementar blockchain*



Nota: Elaboración propia.

## **b. Explicación del aporte**

Se propone utilizar contratos inteligentes y una red descentralizada para garantizar la integridad de los pagos y reducir los riesgos asociados con el fraude y la manipulación de datos. Además, se busca eliminar intermediarios innecesarios y agilizar los procesos de liquidación. Esta implementación beneficiará tanto a los comerciantes como a los consumidores, brindando una experiencia de pago más segura y confiable.

La propuesta está compuesta por las siguientes fases:

### **1. Capacitación y selección del equipo de trabajo.**

La selección y capacitación de un equipo de trabajo para implementar blockchain requiere un enfoque cuidadoso y estratégico, además de una sólida experiencia en el funcionamiento de cadena de bloques y alto conocimiento del sistema de pago en línea.

Para la selección de este personal es importante identificar los roles necesarios para el proyecto de implementación de blockchain, como desarrolladores de blockchain, especialistas en seguridad, analistas de datos, gerentes de proyecto, entre otros.

Adicional se debe proporcionar capacitación y desarrollo continuo a los miembros del equipo en áreas relevantes. Esto puede incluir cursos de formación en blockchain, talleres de desarrollo de habilidades y oportunidades de aprendizaje en el trabajo.

Finalmente es necesario comunicar claramente los objetivos del proyecto y las expectativas de desempeño a todo el equipo.

## **2. Selección de la plataforma blockchain.**

Al evaluar diferentes plataformas blockchain para su implementación en pasarelas de pago, es fundamental llevar a cabo un análisis exhaustivo que considere una serie de factores críticos más allá de la escalabilidad, la seguridad y el costo de operación. Además de estos elementos fundamentales, también es esencial evaluar la capacidad de la plataforma para cumplir con los requisitos regulatorios y de cumplimiento normativo, especialmente en el sector financiero, donde la seguridad y la integridad de los datos son de suma importancia.

Otro aspecto clave a considerar es la interoperabilidad de la plataforma blockchain con otros sistemas y tecnologías utilizados en las pasarelas de pago, como los sistemas de gestión de riesgos, los sistemas de liquidación y los sistemas de gestión de identidades. Una integración fluida y eficiente con estas tecnologías existentes es esencial para garantizar un proceso de pago sin problemas y una experiencia de usuario óptima.

Además, es importante evaluar la comunidad y el ecosistema que rodea a cada plataforma blockchain. Una comunidad activa y comprometida puede proporcionar soporte técnico, actualizaciones regulares y nuevas funcionalidades que impulsen la innovación y mejoren la seguridad de la plataforma a lo largo del tiempo.

Asimismo, se debe considerar la madurez y la estabilidad de la plataforma, así como su historial de desempeño en aplicaciones similares en el pasado. Una plataforma con un historial probado de éxito en aplicaciones de pasarelas de pago puede inspirar mayor confianza y reducir el riesgo de problemas potenciales durante la implementación y el funcionamiento en producción.

## **3. Diseño de la arquitectura de blockchain.**

Al definir una arquitectura de blockchain que se alinee con los procesos existentes de las pasarelas de pago, es esencial considerar una serie de elementos adicionales que garantizarán una integración fluida y eficiente con los sistemas ya establecidos. Además de identificar los nodos de la red y definir los contratos inteligentes, es crucial abordar la interoperabilidad con sistemas externos, la escalabilidad y la seguridad de la arquitectura.

En primer lugar, la interoperabilidad con sistemas externos es fundamental para asegurar que la plataforma blockchain pueda comunicarse de manera efectiva con otros sistemas utilizados en las pasarelas de pago, como los sistemas de gestión de riesgos, los sistemas de liquidación y los sistemas de gestión de identidades. Esto puede implicar la implementación de interfaces estandarizadas y la utilización de protocolos de comunicación comunes para facilitar la transferencia de datos y la ejecución de procesos entre los diferentes sistemas.

Además, la escalabilidad de la arquitectura de blockchain es un factor crítico para considerar, especialmente en el contexto de las pasarelas de pago, donde se pueden procesar grandes volúmenes de transacciones en tiempo real. Es importante diseñar una arquitectura que pueda manejar eficientemente picos de carga de transacciones sin comprometer el rendimiento o la velocidad de procesamiento.

En cuanto a la seguridad, es fundamental implementar medidas robustas para proteger los datos y las transacciones en la plataforma blockchain. Esto puede incluir la implementación de mecanismos de autenticación y autorización sólidos, la encriptación de datos sensibles y la utilización de técnicas avanzadas de detección y prevención de intrusiones para mitigar los riesgos de seguridad.

Finalmente, es importante diseñar la arquitectura de blockchain con la capacidad de adaptarse y evolucionar con el tiempo a medida que cambian los requisitos y las necesidades del negocio. Esto puede implicar la utilización de arquitecturas modulares y flexibles que permitan la incorporación de nuevas funcionalidades y la actualización de componentes existentes de manera eficiente y sin interrupciones en el servicio.

#### 4. **Desarrollo e implementación piloto.**

Es importante llevar a cabo una serie de actividades adicionales para maximizar el éxito del piloto y garantizar su funcionalidad y seguridad en un entorno controlado.

En primer lugar, se debe realizar un análisis detallado de los requisitos del piloto, incluyendo los casos de uso específicos que se probarán, los datos y transacciones involucradas, y los objetivos de rendimiento y seguridad que se esperan alcanzar. Esto ayudará a definir claramente el alcance y los objetivos del piloto, así como a guiar el diseño y desarrollo de la solución blockchain.

Una vez que se hayan establecido los requisitos del piloto, se procederá con el desarrollo e implementación de la solución en un entorno controlado. Esto puede implicar la configuración de una red blockchain privada o de prueba que simule el entorno de producción, pero que permita un mayor control y supervisión durante el proceso de prueba.

Durante la implementación del piloto, es crucial realizar pruebas exhaustivas para garantizar su funcionalidad y seguridad. Esto puede incluir pruebas de integración con sistemas externos, pruebas de rendimiento para evaluar la capacidad de la solución para manejar cargas de trabajo esperadas, y pruebas de seguridad para identificar y mitigar posibles vulnerabilidades y riesgos.

Además, es importante involucrar a todas las partes interesadas relevantes en el proceso de prueba del piloto, incluyendo a los usuarios finales, los equipos de desarrollo y operaciones, y cualquier otro grupo que pueda verse afectado por la implementación de la solución blockchain. La retroalimentación y la colaboración de estas partes interesadas pueden ser invaluable para identificar problemas y oportunidades de mejora durante el proceso de prueba.

Finalmente, una vez que se haya completado el piloto y se hayan realizado todas las pruebas necesarias, se deben analizar los resultados y evaluar la viabilidad y eficacia de la solución propuesta. Esto puede implicar comparar los resultados obtenidos durante el piloto con los objetivos establecidos inicialmente y tomar decisiones informadas sobre el siguiente paso a seguir, ya sea continuar con la implementación a gran escala, realizar ajustes adicionales, o descartar la solución por completo.

## 5. Lanzamiento y monitoreo continuo.

Una vez que el piloto ha demostrado su eficacia en un entorno controlado, el siguiente paso es implementar la solución de blockchain para pasarelas de pago en un entorno de producción. Sin embargo, este proceso de implementación requiere una cuidadosa planificación y gestión para garantizar una transición fluida y exitosa.

En primer lugar, es crucial llevar a cabo una planificación detallada de la implementación, que incluya la definición de un cronograma claro y realista, la asignación de recursos adecuados y la identificación de posibles riesgos y desafíos. Esto ayudará a garantizar que la implementación se realice de manera ordenada y eficiente, minimizando el riesgo de interrupciones en el servicio.

Una vez que se haya completado la planificación, se procederá con la implementación de la solución de blockchain en el entorno de producción. Esto puede implicar la configuración y puesta en marcha de la red blockchain, la migración de datos y procesos existentes a la nueva plataforma, y la integración con sistemas externos y proveedores de servicios.

Durante la implementación, es importante monitorear de cerca el rendimiento de la solución y realizar ajustes según sea necesario para optimizar su funcionamiento. Esto puede incluir la identificación y resolución de problemas técnicos, la optimización de la configuración de la red blockchain y la implementación de mejoras de seguridad y rendimiento.

Además, es esencial proporcionar capacitación y soporte adecuados a los usuarios finales y al equipo de operaciones para garantizar una adopción exitosa de la nueva plataforma. Esto puede incluir la elaboración de materiales de capacitación, la realización de sesiones de capacitación práctica y la provisión de soporte técnico continuo.

Una vez que la solución de blockchain esté completamente implementada y operativa en el entorno de producción, es importante continuar monitoreando su rendimiento y realizando ajustes según sea necesario para garantizar su eficacia a largo plazo. Esto puede incluir la realización de auditorías periódicas de seguridad, la implementación de actualizaciones de software y la evaluación continua del rendimiento y la satisfacción

del usuario. En resumen, la implementación exitosa de la solución de blockchain para pasarelas de pago en producción requiere una planificación cuidadosa, una ejecución precisa y un monitoreo continuo para garantizar su éxito a largo plazo.

## **6. Educación y concienciación sobre seguridad**

La tecnología blockchain, aunque prometedora, es relativamente nueva y su adopción generalizada requiere un esfuerzo significativo en educación y concienciación tanto para los usuarios finales como para los comerciantes y proveedores de servicios. Para alcanzar una adopción exitosa, es esencial que todas las partes involucradas comprendan profundamente los beneficios y el funcionamiento de esta tecnología innovadora.

Los comerciantes y proveedores de servicios necesitan educación y concienciación sobre la tecnología blockchain para comprender cómo puede mejorar sus operaciones y ofrecer un mayor valor a sus clientes. Esto puede incluir capacitación sobre cómo integrar la tecnología blockchain en sus sistemas existentes, cómo aprovechar los contratos inteligentes para automatizar procesos y reducir costos, y cómo utilizar la tecnología para mejorar la seguridad y la confianza en sus transacciones.

Además de la educación, es importante fomentar un diálogo abierto y colaborativo entre todas las partes interesadas para discutir los desafíos y oportunidades asociados con la adopción de la tecnología blockchain. Esto puede incluir la organización de eventos de sensibilización, seminarios y talleres donde se puedan compartir experiencias, mejores prácticas y lecciones aprendidas.

Al implementar esta propuesta de seguridad blockchain, se puede mejorar la confianza de los usuarios, proteger los datos financieros y reducir el riesgo de fraudes y ataques cibernéticos.

### **c. Estrategias y/o técnicas**

#### **Uso y aplicación de cadena de bloques**

Se investiga diferentes fuentes sobre los usos que se le han dado a blockchain y se evalúa ciertas compañías que utilizan esta tecnología. Esta investigación se lleva a cabo con el objetivo de identificar usos y prácticas destacadas que puedan sugerir formas de mitigar los riesgos asociados con los pagos en línea, tal como se han descrito previamente.

Partiendo de los objetivos específicos se ha desarrollado una propuesta que detalla los pasos necesarios para adaptar la cadena de bloques en el proceso de transacciones en pasarelas de pago.

### **Análisis de uso de la tecnología blockchain aplicada en otras empresas**

El uso de blockchain se extiende a diversas áreas, desde las finanzas hasta la cadena de suministro y la atención médica. En las finanzas, blockchain se utiliza para realizar transacciones seguras y transparentes, eliminando la necesidad de intermediarios. En la cadena de suministro, se emplea para rastrear el movimiento de productos desde el fabricante hasta el consumidor, lo que mejora la transparencia y la eficiencia. En la atención médica, se utiliza para mantener registros médicos seguros y precisos, lo que facilita el intercambio de información entre proveedores de atención médica y pacientes. Otros usos incluyen la gestión de identidad, la votación electrónica, la gestión de derechos de autor y la trazabilidad de alimentos, entre otros. (Batz, 2021)

En resumen, blockchain está siendo utilizado en una amplia gama de industrias y sectores para mejorar la seguridad, la transparencia y la eficiencia de los procesos. Blockchain demuestra ser adaptable y beneficioso en múltiples aplicaciones empresariales, proporcionando seguridad, seguimiento, inalterabilidad, visibilidad en tiempo real y un alto nivel de confianza.

### **2.3 Valoración de la propuesta**

La propuesta se llevó a cabo con el acompañamiento y valoración de dos especialistas en el área de seguridad de datos y ciberseguridad. Los expertos consideran que una propuesta de aplicación de blockchain en transacciones de pasarelas de pago es una idea de valor. La tecnología blockchain ofrece varias ventajas que podrían mejorar significativamente la seguridad, la transparencia y la eficiencia de las transacciones en las pasarelas de pago.

Sin embargo, es importante tener en cuenta que la implementación exitosa de blockchain en las pasarelas de pago requerirá una cuidadosa planificación, desarrollo y colaboración entre diversas partes interesadas. Además, deben abordarse desafíos como la escalabilidad, la interoperabilidad y la regulación para garantizar el éxito a largo plazo de esta propuesta. En conclusión, aunque hay desafíos por superar, la aplicación de blockchain en transacciones de pasarelas de pago tiene el potencial de generar un valor significativo para la industria y los usuarios.

Los datos y criterios descritos por los especialistas se encuentran descritos en el Anexo 1.

## 2.4 Matriz de articulación de la propuesta

La Tabla 1 sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos.

**Tabla 1.**

*Matriz de articulación*

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Definición de un equipo de especialistas en seguridad y blockchain.	Criterio propio y de especialistas.	Observación directa	Comparación con otras propuestas enfocadas en la aplicación de procesos para mejorar la seguridad en aplicaciones web.	Este eje se considera fundamental para una buena implementación de la propuesta.	Listas de verificación
Análisis de requerimientos	<b>Título:</b> La ingeniería de requerimientos y su importancia en el desarrollo de proyectos de software.	Investigación bibliográfica	Identificación por fuentes de información relevantes.	Todo proceso que implique un nuevo desarrollo debe pasar por una fase en donde se analicen los requerimientos, para el presente proyecto es importante definir estos	Investigación basada en repositorios institucionales.

	<b>Autor:</b> Michael Arias Chaves.			requisitos junto con el equipo de trabajo.	
Selección de la plataforma blockchain.	<b>Título:</b> Comparison of blockchain platforms.  <b>Autores:</b> Tsung-Ting Kuo, Hugo Zavaleta Rojas, Lucila Ohno-Machado.	Investigación exploratoria	Análisis de la propuesta con respecto a la aplicación de blockchain en otras áreas.	Una plataforma blockchain proporciona un entorno en el cual se pueden crear, desarrollar y ejecutar aplicaciones descentralizadas. Estas plataformas ofrecen una infraestructura tecnológica que permite a los desarrolladores construir soluciones basadas en blockchain lo cual facilita la implementación de la propuesta al eliminar la necesidad de crear una cadena de bloques desde cero.	Revisión de la literatura.
Capacitación del personal	Criterio propio y de especialistas.	Observación directa	Comparación con otras propuestas enfocadas en	La capacitación en blockchain fomenta la	Validación de expertos

			la aplicación de procesos para mejorar la seguridad en aplicaciones web.	innovación y la creatividad dentro de la empresa al presentar nuevas formas de abordar los problemas empresariales. El personal capacitado puede proponer soluciones basadas en blockchain que mejoren la eficiencia, la transparencia y la seguridad de los procesos existentes.	
Desarrollo e implementación piloto	<b>Título:</b> Análisis de pertinencia de una solución de diseño de bloques de seguridad en transacciones descentralizadas para el gobierno electrónico ecuatoriano.	Investigación bibliográfica	Basado en proyectos que implican la implementación de blockchain en diferentes áreas.	Este eje es esencial ya que conlleva la implementación técnica en un ambiente de pre-producción que permitirá validar los requerimientos definidos por el equipo de trabajo.	Búsqueda, recopilación, revisión y análisis de aplicación de cadena de bloques en otras áreas.

	<p><b>Autores:</b> Andres Ramos, Pablo Recalde</p>				
<p>Diseño de la arquitectura de blockchain</p>	<p><b>Título:</b> Blockchain en el sector financiero y la seguridad en las transacciones bancarias y bitcoin Blockchain in the financial sector and security in banking and bitcoin transactions</p> <p><b>Autor:</b> Domingo Iván Yax Batz</p>	<p>Investigación exploratoria</p>	<p>Investigación cualitativa</p>	<p>La arquitectura está diseñada para garantizar la integridad de los registros y la seguridad de las transacciones utilizando tecnologías como la criptografía y la descentralización, por lo que es importante trabajar en el diseño de la misma.</p>	<p>Análisis de contenido</p>

<p>Lanzamiento y monitoreo continuo</p>	<p><b>Título:</b> Blockchain en el sector financiero y la seguridad en las transacciones bancarias y bitcoin Blockchain in the financial sector and security in banking and bitcoin transactions</p> <p><b>Autor:</b> Domingo Iván Yax Batz</p>	<p>Observación directa</p>	<p>Fundamentos teóricos y de especialistas</p>	<p>La séptima fase describe la puesta en marcha de la integración y el constante monitoreo que permite una mejora continua del rendimiento, la seguridad y la eficiencia.</p>	<p>Observación y registro</p>
<p>Educación y concienciación sobre seguridad</p>	<p><b>Título:</b> Importancia de la seguridad informática y ciberseguridad en el mundo actual</p>	<p>Investigación bibliográfica</p>	<p>Basado en la investigación de los beneficios de capacitación y concienciación sobre seguridad.</p>	<p>Se espera que las personas adquieran un mayor conocimiento sobre los diversos riesgos de seguridad que enfrentan, incluyendo amenazas cibernéticas, fraudes,</p>	<p>Investigación basada en el sustento teórico.</p>

	<b>Autor:</b> Gamboa Suarez, Jose Luis			robos de identidad, entre otros	
--	---	--	--	------------------------------------	--

Fuente: Elaboración propia

## CONCLUSIONES

Los fundamentos teóricos sobre seguridad y blockchain encontrados durante el desarrollo de la investigación permiten valorar la propuesta desarrollada ya que brinda un alto grado de confianza al recurrir a fuentes de expertos y libros que profundizan la aplicación de blockchain en diversas áreas fuera del ámbito de bitcoin.

Las vulnerabilidades y amenazas detectadas en el flujo de una transacción bancaria a través de una pasarela de pago permitieron comprender que actualmente las empresas proveedoras de este servicio se enfrentan a grandes desafíos y posibilidades de ser atacados debido al manejo de información sensible y cotizada de los usuarios que usan el comercio electrónico.

Al diseñar una propuesta que promueva la aplicación de blockchain como técnica de seguridad en el proceso de transacciones de pago en línea, hemos trazado un camino hacia la mejora de la seguridad y la confianza en el comercio digital. Esta propuesta no solo ofrece una solución innovadora y eficaz para abordar los desafíos de seguridad en las transacciones en línea, sino que también allana el camino para una mayor adopción y aceptación de la tecnología blockchain en el ámbito financiero y comercial. Al implementar esta propuesta, podemos trabajar hacia un futuro donde las transacciones en línea sean más seguras, eficientes y transparentes para todos los usuarios.

Al valorar el diseño de la propuesta con el criterio de especialistas en seguridad, se asegura un enfoque sólido y bien fundamentado para abordar los desafíos de seguridad en el proceso de transacciones en línea. La retroalimentación y validación de estos expertos no solo garantizan la integridad y eficacia de la propuesta, sino que también fortalece la confianza en su capacidad para mitigar riesgos y proteger los datos de manera efectiva. Al integrar las perspectivas y recomendaciones de estos profesionales, se posiciona a la propuesta como una solución robusta y confiable para mejorar la seguridad en el comercio electrónico y las transacciones en línea.

## RECOMENDACIONES

Para complementar los fundamentos teóricos encontrados durante la investigación, se sugiere explorar casos de estudio y ejemplos prácticos de implementaciones exitosas de blockchain en diferentes industrias y países. Esto ayudará a enriquecer la propuesta desarrollada al ofrecer ejemplos concretos de cómo la tecnología blockchain puede ser aplicada de manera efectiva fuera del ámbito de Bitcoin.

Profundizar el estudio de cadena de bloques en áreas de mejoras de procesos, para aprovechar la versatilidad de aplicación en varios sectores como educación, salud, logística, finanzas, entre otros.

Se puede utilizar la presente propuesta de aplicación de blockchain en otras áreas internas que manejen datos sensibles o que la seguridad sea fundamental.

Es importante seguir involucrando a especialistas en seguridad durante todas las etapas del proceso, incluso después de la implementación de la propuesta. Esto garantizará que se mantenga actualizada y adaptable a los cambios en el panorama de seguridad cibernética. Además, se deberían establecer mecanismos para recopilar y evaluar continuamente la retroalimentación de los usuarios finales, lo que permitirá identificar áreas de mejora y garantizar que la propuesta siga siendo relevante y efectiva a lo largo del tiempo.

## BIBLIOGRAFÍA

- 101 Blockchains, "20 Empresas Que Están Implementando La Tecnología Blockchain," 2022, [Online]. Available: <https://101blockchains.com/es/empresas-implementandoblockchain/>.
- Amo Filvà, D., Alíer Forment, M., García-Peñalvo, F. J., Fonseca Escudero, D., & Casañ Guerrero, M. J. (2020). Privacidad, seguridad y legalidad en soluciones educativas basadas en Blockchain: Una Revisión Sistemática de la Literatura. RIED. Revista Iberoamericana de Educación a Distancia, 2020, Vol. 23, No 2.
- Batz, D. I. Y. (2021). Blockchain en el sector financiero y la seguridad en las transacciones bancarias y bitcoin. CyberSecurity, 20.
- Chaves, M. A. (2005). La ingeniería de requerimientos y su importancia en el desarrollo de proyectos de software. InterSedes: Revista de las Sedes Regionales, 6(10), 1-13.
- Cortés, R. J. (2012). Coaching en el desarrollo profesional docente. Fases formativas y procesos metodológicos de investigación. Revista electrónica interuniversitaria de formación del profesorado, 15(4), 101-112.
- Fuentes Morales D., Flores Velazquez, J., Roblero R. (2022). La web de las cosas (WoT) para monitoreo y control de biosistemas con aplicaciones prácticas en Agricultura Urbana (AgUrban).
- Hernández, E. F. T., Canizales, R. R., & Páez, A. V. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual. Misión Jurídica: Revista de derecho y ciencias sociales, 14(20), 142-158.
- Hlaing, K. M., & Nyaung, D. E. (2019, November). Electricity billing system using Ethereum and firebase. In 2019 International Conference on Advanced Information Technologies (ICAIT) (pp. 217-221). IEEE.
- Kuo, T. T., Zavaleta Rojas, H., & Ohno-Machado, L. (2019). Comparison of blockchain platforms: a systematic review and healthcare examples. Journal of the American Medical Informatics Association, 26(5), 462-478.
- Lozano, S. J. C. (2015). Comercio electrónico: Importancia de la seguridad en las transacciones electrónicas, amenazas y soluciones a implementar. Revista Empresarial, 9(35), 8-14.
- Luna Luna, Á. (2022). Blockchain para gestionar vulnerabilidades y exposiciones comunes en sistemas de Smart Grid federados-VECsg.
- Mougayar, W. (2016). The business blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons.
- Ramos Rodríguez, A. R. (2023). Análisis de pertinencia de una solución de diseño de bloques de seguridad en transacciones descentralizadas para el gobierno electrónico ecuatoriano (Master's thesis, Quito, Ecuador: Editorial UISRAEL).

- Salinas Guarderas, H. O. (2022). Análisis comparativo entre las pasarelas de pago (Placetopay y PayPal) para forjar EPP (Bachelor's thesis, Babahoyo: UTB-FAFI. 2022).
- Salinas Tamayo, E., Barrientos Correa, A. F., & Quiroz Osorio, J. F. (2021). Pasarelas de pago en Colombia, un mercado cambiante y altamente competitivo.
- Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.
- Vidal, N., & Isidro, P. (2022). Identidad digital en pasarelas de pago.
- Y. J. R. Altamirano and S. Bayona Oré, "Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento," RISTI - Rev. Iber. Sist. e Technol. Inf., vol. 2017, no. 25, pp. 112–134, 2017.

## ANEXOS

A continuación, se detalla los instrumentos utilizados en el trabajo de titulación.

### ANEXO 1

#### VALIDACIÓN DE EXPERTOS

##### INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

##### INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de aplicación de blockchain en transacciones de pasarelas de pago en Ecuador para mejorar su seguridad.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Fabricio Xavier Pilicita Garrido

Título obtenido
Ingeniero en Sistemas
Cédula de Identidad
1724528094
E- mail
fabricio.pilicita1991@gmail.com
Institución de Trabajo
Equifax
Cargo
Analista de seguridad
Años de experiencia en el área
Tres años

**Instructivo:**

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

**Tema:** Propuesta de aplicación de blockchain en transacciones de pasarelas de pago en Ecuador para mejorar su seguridad.

Indicador	Descripción	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
<b>Impacto</b>	El alcance que tendrá la propuesta y su representatividad en la generación de valor		X			
<b>Aplicabilidad</b>	La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables		X			
<b>Conceptualización</b>	La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada	X				
<b>Actualidad</b>	Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta	X				
<b>Calidad Técnica</b>	Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios		X			
<b>Factibilidad</b>	El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles		X			
<b>Pertinencia</b>	La contundencia y conveniencia de la propuesta para solucionar el problema planteado.			X		
<b>Total</b>		<b>2</b>	<b>4</b>	<b>1</b>	<b>0</b>	<b>0</b>

**Observaciones:**

Siempre que una empresa maneja datos sensibles es importante planear metodologías o procesos que ayuden a mitigar los riesgos de modificación, mal uso o robo de estos datos. La propuesta planteada es una guía pensada para empresas proveedores de pagos en línea, las mismas deberían analizar la posibilidad de implementar el mejoramiento de la seguridad a través de la cadena de bloques propuesta por el autor del proyecto en mención.

**Recomendaciones**

La implementación de blockchain podría ofrecer una mayor transparencia y confianza en las transacciones de pasarelas de pago ya que proporcionan un registro inmutable y descentralizado de todas las transacciones realizadas. Esto ayudaría a prevenir fraudes, mejorar la integridad de los datos financieros y proteger la información de los clientes de manera más efectiva. Sin embargo, mi recomendación es tener en cuenta que la adopción exitosa de blockchain en este contexto requerirá una cuidadosa consideración de factores como la escalabilidad, la interoperabilidad y los costos asociados.

Lugar, fecha de validación: Quito, 2 de marzo del 2024



---

Firma del especialista

**INSTRUMENTO DE VALIDACIÓN**

**UNIVERSIDAD TECNOLÓGICA ISRAEL  
ESCUELA DE POSGRADOS "ESPOG"**

**MAESTRÍA EN SEGURIDAD INFORMÁTICA  
INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA**

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de aplicación de blockchain en transacciones de pasarelas de pago en Ecuador para mejorar su seguridad.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Ivette Castrillón

<b>Título obtenido</b>
Master en Ciberseguridad
<b>Cédula de Identidad</b>
1722214945
<b>E- mail</b>
<a href="mailto:ivetcastril@hotmail.com">ivetcastril@hotmail.com</a>
<b>Institución de Trabajo</b>
Nuvei/Paymentez
<b>Cargo</b>
Especialista en seguridad
<b>Años de experiencia en el área</b>
3 años

**Instructivo:**

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una **X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

**Tema:** Propuesta de aplicación de blockchain en transacciones de pasarelas de pago en Ecuador para mejorar su seguridad.

<i>Indicador</i>	<i>Descripción</i>	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
<b>Impacto</b>	<i>El alcance que tendrá la propuesta y su representatividad en la generación de valor</i>	X				
<b>Aplicabilidad</b>	<i>La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables</i>		X			
<b>Conceptualización</b>	<i>La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada</i>	X				
<b>Actualidad</b>	<i>Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta</i>	X				
<b>Calidad Técnica</b>	<i>Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios</i>		X			
<b>Factibilidad</b>	<i>El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles</i>			X		
<b>Pertinencia</b>	<i>La contundencia y conveniencia de la propuesta para solucionar el problema planteado.</i>		X			
<b>Total</b>		<b>3</b>	<b>3</b>	<b>1</b>		

**Observaciones:**

Como consultora de la señorita Kerly Naranjo considero factible la propuesta planteada. Cada vez son mas las empresas que adoptan blockchain para mejorar la seguridad y distribución de los datos. Aunque la tecnología es poco conocida por los usuarios que realizan compras en línea, el beneficio que ellos obtienen es significativo.

**Recomendaciones**

Con el fin de resaltar los beneficios de la implementación de bloques de datos, recomiendo generar conciencia en las empresas que proveen botón de pago con tarjeta de crédito, sobre la importancia de conocer e incursionar en nuevas tecnologías que aporten a la seguridad y calidad de datos.

**Lugar, fecha de validación:** Quito, 28 de febrero del 2024

  
Firma del especialista