UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO DE SISTEMAS

CARRERA:

INGENIERÍA DE SISTEMAS

TEMA:

"MODELO DE SEGURIDAD DE INFORMACIÓN BASADO EN LA TECNOLOGÍA BLOCKCHAIN PARA LOS PROCESOS DEL SERVICIO DE RENTAS INTERNAS DEL ECUADOR"

AUTOR:

David Antonio Bajaña Troya

TUTOR:

Msg. Máximo Giovani Tandazo Espinoza

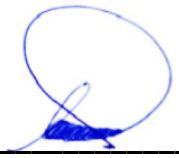
Julio 2021

GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **DAVID ANTONIO BAJAÑA TROYA**, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

FIRMA ESTUDIANTE
Nombre: DAVID ANTONIO BAJAÑA TROYA
CI. 0928830736



FIRMA TUTOR
Nombre: MAXIMO GIOVANI TANDAZO ESPINOZA
CI. 0916028921

Modelo de seguridad de información basado en la tecnología Blockchain para los procesos del Servicio de Rentas Internas del Ecuador

Máximo Giovani Tandazo Espinoza[1[0000-0002-8844-9384]] and David Antonio Bajaña Troya [1[0000-0003-2012-7634]]

[1] Department of Computer Science, Universidad Politécnica Salesiana Sede Guayaquil, Ecuador, Chamber 227 y 5 de junio
dtandazo@ups.edu.ec, dbajanat@est.ups.edu.ec

Abstract. Se analizó información de las referencias sobre blockchain y procesos de impuestos para dar una alternativa de seguridad a los datos. El problema es la información incompleta de datos almacenados, la actualización de datos ya aprobados que genera desconfianza, entrega de documentos con datos falsificados; los documentos alterados o dañados, alta latencia en los entornos de datos centralizados son otros inconvenientes. El objetivo es proponer un modelo de seguridad de información para un proceso de declaración de impuestos del Servicio de Rentas Internas basado en la tecnología blockchain. La metodología que se aplicó es la investigación exploratoria y método deductivo para analizar la información de las referencias que contienen la tecnología blockchain, Hyperledger, Ethereum y los procesos del Servicio de Rentas Internas del Ecuador. Esta investigación resultó en un Análisis de los participantes públicos y privados para un esquema de seguridad en blockchain, Conceptualización de una arquitectura híbrida para los procesos de declaración de impuestos, y Evaluación del rendimiento de la arquitectura híbrida a través de una simulación. Se concluyó que el modelo propuesto formado por los participantes, arquitectura híbrida en Hyperledger/Ethereum, funciones y los algoritmos, brindan un mayor nivel de seguridad a la información que se origina en los contribuyentes y es procesada por la entidad estatal a través de la tecnología blockchain que mantiene los datos con transparencia, privacidad y seguridad; en las simulaciones teóricas del modelo el menor rendimiento fue 71.02% y máximo rendimiento fue 99.39%; se dedujo que el rendimiento está en función de la cantidad de transacciones que se almacenaron versus la cantidad de transacciones que se enviaron a la red híbrida.

Keywords: Blockchain, Tax, Distributed architecture, Hyperledger, Ethereum, Smart Contract.

1 Introducción

Los impuestos son una parte del financiamiento de un país que un gobierno utiliza para proyectos de educación, salud, infraestructura, entre otros; los gobiernos se encargan crear políticas para hacer cumplir nuestras obligaciones fiscales, mientras la dinámica de los negocios es cada vez mayor; las TICs asisten como mecanismo para que los contribuyentes declaren y paguen sus impuestos de manera correcta y ordenada[1].

Los procesos cada vez más se basan en datos y la información crece, los estados de las transacciones son de interés para los participantes; la información en bases de datos tradicionales que sirven para análisis, diagnóstico y predicciones, sin embargo, existe el riesgo que los datos sean alterados en cualquier momento a lo largo del tiempo; es necesario que los datos mantengan su integridad para mantener la confianza en los procesos y participantes. Es difícil generar la confianza de todos los contribuyentes porque todo son desconocidos; si el gobierno desconfía del contribuyente, las inspecciones físicas y frecuentes generan costos para aplicar las normas legales[2].

Los sistemas y bases de datos tradicionales que utilizan el anonimato tienen un nivel bajo de protección de datos; existe el riesgo de acceso no autorizado e identificación de información

confidencial[3]. El gobierno de Indonesia emitió un reglamento para la gestión de datos porque los datos recopilados eran equívocos, desactualizados, no integrados, no rastreables, el acceso y compartición eran difíciles[4]; los gobiernos de India, Georgia, Honduras y Sweden exploran proyectos en para asegurar la integridad de datos en sectores como tierras e impuestos, la opción adoptada por ellos fue Blockchain[5]; el gobierno de India y Dubái utilizan tecnología blockchain[6].

Blockchain (BK) es una base de datos distribuida, existe una réplica en cada uno de los participantes de la red BK, las transacciones se almacenan en bloques inmutables; al momento de actualizar un dato se adiciona un nuevo bloque; BK utiliza un método de consenso replicado en los participantes para aprobar las transacciones[1]. BK utiliza algoritmos criptográficos para garantizar la integridad de una transacción, la transacción inicia con la firma del propietario, se envía y se valida en todos los nodos, cada nodo debe dar su aval para el guardado de la transacción; dicho guardado es a través de un consenso en la red BK[2].

Smart Contract (SC) es un código de programa para la gestión de las transacciones hacia el conjunto de bloques en un consenso descentralizado; cada participante de la red BK tiene una copia del SC y ejecuta su propio SC; además se comprueban el estado y actualizaciones de las transacciones[7]. Las lógicas del negocio que son complejas están en el SC; además el SC se actica desde eventos externos pre diseñados[2]. Ethereum es una aplicación descentralizada, aquí el usuario utiliza Eth para pagar la información que guarda y procesa[7]; los SC son de propósito general[2]. Hyperledger es una cadena para acceso privado a los bloques de datos, a esta información que es confidencia sólo tienen acceso los participantes especificados en el consorcio[6].

Existen dos tipos de BK Público y BK Privado; BK Público es una red de confianza cero, cualquiera se une, lee y escribe en el ledger; el BK privado todos los participantes forman un consenso en la red y confianza, además se consume menos recursos en el procesamiento de la transacción[4].

Ventajas de utilizar BK: son bajo mantenimiento de aplicaciones BK, menos confirmaciones en las transacciones, menor tiempo de procesamiento[7]; confianza entre los participantes, transacciones a nivel de confianza cero, transacciones auditables e inmutables[2]. Desventaja: Falta de usuarios privilegiados en una red BK pública y cualquier anónimo puede acceder a esa red como participante; problemas de escalabilidad debido a la creciente dimensión de datos, tasa transaccional y latencia en la transmisión; la cantidad de participantes en el protocolo de consenso disminuye el tiempo de confirmación de una transacción[2]. En ISO/IEC 27001:2013 se nombra la Confidencialidad, Integridad y Disponibilidad como componentes de protección y aseguramiento de la información; la confidencialidad evita el robo o publicación de información; la integridad mantiene sin cambio los datos, y la disponibilidad mantiene el acceso del propietario a su propia información[4].

En Ecuador el Servicio de Rentas Internas (SRI) es una organización pública encargada de la gestión tributaria dentro de la constitución de la república; entre los servicios que ofrece la entidad están: consulta de registro de contribuyentes, gestión de facturas físicas y electrónicas, declaraciones de impuestos y anexos; gestión de pagos, deudas, devoluciones y certificados[8].

El problema es la información incompleta de datos almacenados, la actualización de datos ya aprobados que genera desconfianza, entrega de documentos con datos falsificados; los documentos alterados o dañados, alta latencia en los entornos de datos centralizados son otros inconvenientes.

¿Por qué es necesario un enfoque de Blockchain en un proceso de declaración de impuestos para el Servicio de Rentas Internas del Ecuador?

Para que contribuyentes y gobierno tengan información de impuestos en un entorno seguro y privado; minimizar esfuerzos en la gestión de información fiscal, tener un potencial tecnológico aplicado a información en el desempeño tributario; generar confianza de las declaraciones de los contribuyentes en los administradores tributarios y viceversa.

Motivación: Blockchain es una opción con mayor grado de seguridad y privacidad para los datos, a través de una tecnología confiable en un ambiente distribuido entre los participantes; la descentralización es una alternativa a la información dependiente de autoridades y terceros; mantener la seguridad de la información.

El objetivo es proponer un modelo de seguridad de información para un proceso de declaración de impuestos del Servicio de Rentas Internas basado en la tecnología blockchain.

Se utiliza la investigación exploratoria y método deductivo para analizar la información de las referencias que contienen la tecnología blockchain, Hyperledger, Ethereum y los procesos del Servicio de Rentas Internas del Ecuador.

2 Materiales y Métodos

2.1 Materiales

Blockchain aplicado en la confidencialidad, integridad o disponibilidad de información:

Para mantener de manera inmutables los documentos digitalizados los autores de [1] diseñaron una arquitectura de 3 capas; la primera capa para procesos de auditoria, la segunda capa para interfaces de transacciones, la tercera capa contiene los contratos y bloques; cada participante puede adicionar su parte de SC; la arquitectura la desarrollaron en Ethereum para accesos públicos, y el SC lo desarrollaron en Solidity. Para realizar rastreo inverso, gestión de equipos y eficiencia de los productos fabricados, los autores de [2] propusieron utilizar BK en la gestión de datos; los participantes son proveedores, gobierno, fabrica, distribuidores, vendedores y compradores; además la propuesta abarca elevar la calidad de datos en todos los procesos de fabricación de un producto. Para mantener la seguridad y privacidad en los datos de los contribuyentes y cálculo de impuestos, los autores de [3] realizaron un prototipo que consta de dos partes; la primera parte es administrada por la agencia tributaria, es centralizada y contiene los datos personales de los contribuyentes, esta permitir el anonimato y privacidad de los contribuyentes; la segunda parte es descentralizada y cada contribuyente calcula sus impuestos a través de una interface, luego los datos de impuestos son enviados y validados en la cadena BK; el prototipo fue implementado en Ethereum. Para mantener la integridad de los documentos en registro de terrenos los autores de [5], implementaron una arquitectura en Ethereum para la parte publica e Hyperledger Composer para la parte privada; entre los participantes están los vendedores, compradores, oficina de registros y banco.

Blockchain aplicado en gestión de impuestos:

La autenticación de documentos generados por autoridades de gobierno en India a través de BK privado es una propuesta de [6] en Hyperledger Fabric, HTML y CSS. Para el pago de impuestos por el uso de carreteras a nivel nacional con una previa suscripción, los autores de [7] diseñaron

y desarrollaron una aplicación web en Ethereum; la propuesta tiene creación de moneda, pago del impuesto y suscripción; desarrollado en Solidity y JavaScript. Los autores de [9] diseñaron e implementaron una aplicación informática para el pago de impuestos; el diseño tiene 3 capas, una para participantes, la segunda capa para almacenar los documentos digitalizados, la tercera capa es la red BK en Ethereum y SC con funciones del negocio; para la implementación utilizaron Ethereum VM, Solidity language, Remix IDE. Para el pago de impuestos a través de los bancos, los autores de [10] diseñaron un modelo de recaudación basado en Hyperledger Fabric; los participantes son agencia reguladora de bancos, agencia fiscal de impuestos y bancos privados; los datos del contribuyente junto a clave pública se guardan en la red BK, la agencia reguladora y los bancos utilizan una clave privada para acceder a los datos y realizar el pago; el SC crea o consulta datos de los impuestos y créditos para los pagos de impuestos. BK es utilizado para el almacenamiento seguro de documentos con sus datos, como registro de propiedades, certificados de todo tipo, entre otros; el usuario recibe un ticket con los códigos del documento digital; los autores implementaron la arquitectura con Hyperledger Fabric, una arquitectura de 3 capas, Rest Api y aplicación web[11]. El aseguramiento de documentación oficial en Indonesia y aumento de la eficiencia de actividades en BK privado a través de Hyperledger es una propuesta de [12]; ellos diseñaron una arquitectura de 4 capas, la implementación fue en Go lenguaje, Docker, CouchDB y Bash sobre SO Linux Fedora. Los autores de [13] diseñaron una red BK para las identidades de usuarios en una organización pública; basada en Hyperledger la red mínimo debe tener 2 organizaciones enlazadas a través de un consorcio; la lógica del negocio aplicada a la identidad está en el SC; los datos se encriptan con algoritmo AES; la probabilidad mínima de éxito es 36% y la probabilidad máximo es 99%. Una red BK mixta se propuso para el sistema de datos públicos; la parte pública en Ethereum es para los ciudadanos; la parte privada en Hyperledger está formada por organizaciones públicas; las simulaciones del modelo fueron un promedio de 90% de eficiencia[14].

Otras implementaciones en blockchain

Los autores de [15] implementaron una red basada en Hyperledger, 3 organizaciones, 2 consorcios, 2 canales, 1 ordenador de servicios; un participante tiene 2 ledger, los otros dos tienen un ledger cada uno; además cada canal tiene sus propias reglas de negocio. Para evitar el engaño por parte de clientes o proveedores, en[16] diseñaron un protocolo para suscripción y pagos a través de la nube; esto contienen dos SC para los procesos de suscripción, accesos, recursos y vencimiento; la red BK se implementó en Ethereum con JSON web, REST API y Solidity. Los autores implementaron una red Ethereum una plataforma general en entorno web y en máquina virtual[17]; en la referencia [18] diseñaron y desarrollaron una red Ethereum en una máquina virtual, Node.js, un IDE propietario y Solidity para implementar el SC; el modelo de pago en Ethereum[19] tiene como participantes un banco, clientes y vendedores, aquí la aplicación servidor está en el banco bajo Python; la referencia [20] propone un prototipo para la actualización de reclamos que estén encriptados a través de Ethereum.

2.2 Métodos

Características tecnológicas de blockchain:

Esta tecnología tiene buenas características y beneficios.

- Propiedades: es una arquitectura descentralizada o distribuida, no tiene una autoridad centralizada, los participantes mantienen un consenso sin confiar entre ellos; los datos contenidos en los bloques son

inalterables o inmutables, para esto utiliza algoritmos criptográficos y garantizar la integridad de datos; transparencia a través del acceso público a los participantes; validación de las transacciones a través del protocolo de consenso; trazabilidad de las transacciones generadas en el proceso colaborativo[2].

- Timestamping es una marca de fecha y hora que se codifica en cada bloque, con esto se comprueba la existencia de la transacción en el bloque; Consenso es un acuerdo con confianza cero entre los participantes, cada nodo aprueba la transacción para convertirse en un bloque adicional a la cadena; Seguridad e integridad no se pueden generar transacciones falsas debido a claves privadas y consenso, no existe la eliminación ni actualización de transacciones en los bloques, sólo existe la adición de bloques cifrados y el acceso es a través de certificados[21].

Razones para adoptar blockchain en una organización pública:

- Plataforma Hyperledger: acceso sólo a las entidades autorizadas, codificación para obtener datos de ciudadanos, mantiene la seguridad y privacidad en los datos, ofrece identidad a los participantes[14]; cambios positivos, seguridad de datos en las transacciones, tecnología apropiada para entidad pública o privada, acceso y uso sencillo[22];
- Plataforma Ethereum: permite a los ciudadanos entrar a la red y mantener los datos inmutables[14], ciudadanos pueden utilizar claves públicas [5].

Participantes en la creación de contribuyentes en Ecuador:

Son contribuyentes todas las personas naturales o jurídicas que tienen alguna actividad comercial con o sin fines de utilidades:

- Servicio de Rentas Internas,
- Superintendencia de compañías,
- Banco, Municipio, Registro Mercantil,
- Contribuyentes que declaran sus impuestos, pueden ser personas naturales o personas jurídicas.

Alcance de ésta investigación:

- Aplicar BK en un proceso de declaración de impuestos
- Separar los datos personales y el proceso de impuestos
- El proceso de recaudación de dinero lo continúan los bancos o recaudadores
- Adoptar Ethereum para la parte pública y el anonimato de los contribuyentes
- Adoptar Hyperledger para la parte privada y el consenso entre los participantes
- Estado de la declaración de impuesto puede ser “Pendiente de Pago” o “Pagado”

3 Resultados

En esta fase los resultados son los siguientes:

- Análisis de los participantes públicos y privados para un esquema de seguridad en blockchain.
- Conceptualización de una arquitectura híbrida para los procesos de declaración de impuestos.
- Evaluación del rendimiento de la arquitectura híbrida a través de una simulación.

3.1 Análisis de los participantes públicos y privados para un esquema de seguridad en blockchain.

Para proponer un esquema en blockchain es necesario la formación de los participantes privados en una plataforma Hyperledger separados de los participantes públicos en una plataforma Ethereum, esto se muestra en la Fig. 1.

La plataforma Hyperledger es una red privada formada por cinco organizaciones, a continuación describimos las funciones de cada uno en la red: el Servicio de Rentas realiza las funciones de control de las declaraciones de impuesto a la renta de contribuyentes, confirmar los pagos del contribuyente, aviso de cobro, actualización de la declaración de impuesto; el Registro Mercantil realiza la gestión de trámites, gestión de contratos, documentación judicial, nombramientos y

certificaciones; la Superintendencia de Compañías realiza constitución de la compañía, gestión de informes de auditorías y gestión de las acciones de una compañía; Municipio realiza la gestión de tasa de habilitación, gestión de derecho uso de suelo y gestión de estatutos de la compañía; el banco local localiza el valor del impuesto, capta el pago y envía los datos del pago a la red BK. En esta red todos los participantes tienen un consenso de aceptación de las transacciones, es decir conocen en modo distribuido acerca de las declaraciones de impuestos de los contribuyentes.

La plataforma Ethereum es una red pública formada por todos los contribuyentes que deben declarar sus impuestos al Servicio de Rentas; entre las funciones que afectan a la red BK están: creación de contribuyente, obtención del registro, registrar la declaración del impuesto, registrar de retención de impuestos, y registro de reclamos administrativos.

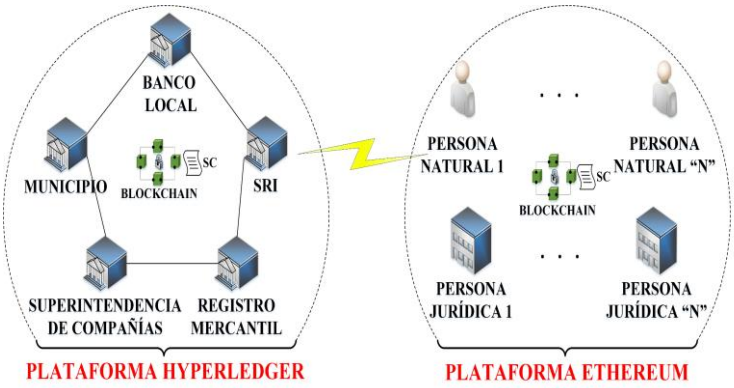


Fig. 1. Participantes públicos y privados.

3.2 Conceptualización de una arquitectura híbrida para los procesos de declaración de impuestos.

La arquitectura propuesta está dividida en Hyperledger y Ethereum como se muestra en la Fig. 2.

La estructura de la red privada Hyperledger contiene los siguientes componentes:

- El Servicio de Rentas es la responsable de crear la red BK, las configuraciones, los servicios, adicionar los participantes a la red, entregar las credenciales a los demás participantes.
- Canal de comunicación sirve de enlace para la red BK, solo los participantes nombrados tienen acceso a este canal
- Consorcio: está formado por las 5 organizaciones nombradas en el esquema de seguridad.
- Ordering Service: el administrador de la red BK crea los participantes en este componente y su configuración.
- Cada participante contiene un certificado de autenticidad, aplicación cliente Hyperledger para acceder al sistema, una copia del SC, y una copia del ledger; cada uno esta enlazado al canal de comunicación.
- Los servicios de membresía: cada Peer contiene una membresía local para su participación en el canal.

La estructura de la red pública Ethereum contiene los siguientes componentes:

- Los contribuyentes pueden acceder a la red Ethereum a través de una aplicación cliente Ethereum, la red contiene Smart Contract para las funciones de los contribuyentes, las claves públicas para los contribuyentes, y el ledger que se será afectado por los contribuyentes.

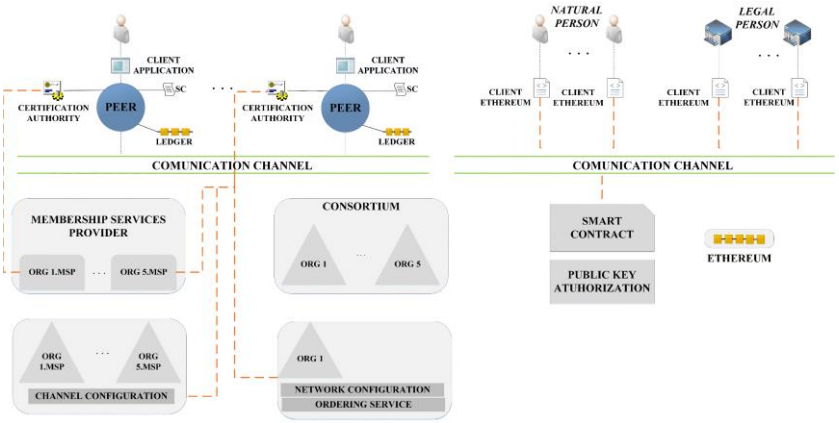


Fig. 2. Arquitectura híbrida en blockchain.

Para la plataforma Hyperledger se propone utilizar HL Composer para el conjunto de datos, HL Fabric para el lenguaje de alto nivel, HL Fabric CA para los certificados; HTML, Javascript y CSS para el lado del cliente[13].

Para la plataforma Ethereum se propone utilizar Ethereum Virtual Machine; Solidity es un lenguaje de alto nivel para desarrollar el SC; Truffle es un framework para desarrollo de aplicaciones en Ethereum; para el cliente se propone HTML, CSS y Javascript[17].

Definición de las funciones del Smart Contract

El SC contiene el código de programa para establecer la lógica del negocio, las funciones son invocadas desde la aplicación cliente o interface; estas funciones leen o actualizan la red BK; la arquitectura contiene 2 redes BK, por esto es necesario definir las funciones para cada red; la Tabla 1 contiene las funciones para la plataforma Hyperledger, la Tabla 2 contiene las funciones para la plataforma Ethereum.

Table 1. Funciones del SC Hyperledger.

Función	Descripción	Responsable
Control de declaraciones	Verificar los datos de facturas en las declaraciones	SRI
Control de impuestos declarados	Verificar montos de las declaraciones a través de auditorías tributarias	SRI
Deterrminar impuesto	Actualizar los valores en la declaración del impuesto en documento sustitutiva	SRI
Crear sustitutiva	Crear o actualizar en una nueva declaración de impuesto	SRI
Aviso pago del impuesto	Crear el comprobante de pago con datos del contribuyente, fecha de emisión, fecha de expiración, tipo de impuesto y valor	SRI
Actualizar estado de la declaración	Actualizar la declaración del impuesto tiene 3 estados: Pendiente de pago o Pagado o Deuda en firma	SRI, Banco
Gestion de trámites	Crear nuevo tramite o actualizar las tasas	R. Mercantil
Gestion de documentacion judicial	Crear o actualizar auditorías o juicios realizados a la compañía	R. Mercantil

Función	Descripción	Responsable
Certificados	Generar y almacenar certificados solicitados por la compañía	R. Mercantil
Gestión de documentos de compañía	Crear o actualizar las escrituras de constitución de la compañía	Sup. de Compañías
Gestión de informes de auditorías	Crear o actualizar los informes de auditorías realizadas a las compañías	Sup. de Compañías
Gestión de las acciones	Crear o actualizar la distribución del capital inicial de la compañía	Sup. de Compañías
Gestión de tasas de habilitacion	Crear, emitir y actualizar los requisitos de funcionamiento en local físico para la compañía o persona natural	Municipio
Gestión de estatutos de la compañía	Crear o actualizar los lineamientos de la compañía o persona natural	Municipio
Buscar valor de impuesto	Localizar en la red el valor de impuesto a pagar por el contribuyente	Banco

Table 2. Funciones del SC Ethereum.

Función	Descripción
Crear contribuyente	Crear o actualizar los datos de un contribuyente
Subir documentos	Subir o actualizar los documentos digitales
Declarar impuesto	Crear el registro de activos, pasivos, ingresos y egresos del contribuyente
Cálculo del impuesto	Operaciones aritméticas de los valores, puede ser valor cero o positivo
Pago de impuesto	Pagar por medio electrónico los valores del impuesto
Enviar estado del impuesto	Enviar a red HL el estado
Enviar declaracion	Enviar a red HL la declaración

Además, para complementar la arquitectura híbrida proponemos dos algoritmos genéricos expresados en diagramas de flujo, para entender mejor la ejecución teórica e interacción entre la red Hyperledger y Ethereum.

En la Fig. 3 el mismo contribuyente se registra en la red Ethereum, los datos se envían a red Hyperledger para validación de acuerdo a su tipo de persona, e intervienen las otras autoridades para revisiones físicas.

En la Fig. 4 el contribuyente ingresa datos de su declaración en la red Ethereum, los datos son enviados a la red Hyperledger con la actualización del estado de pago, al pagar el contribuyente debe realizar transacción electrónica y se envía el estado de pago.

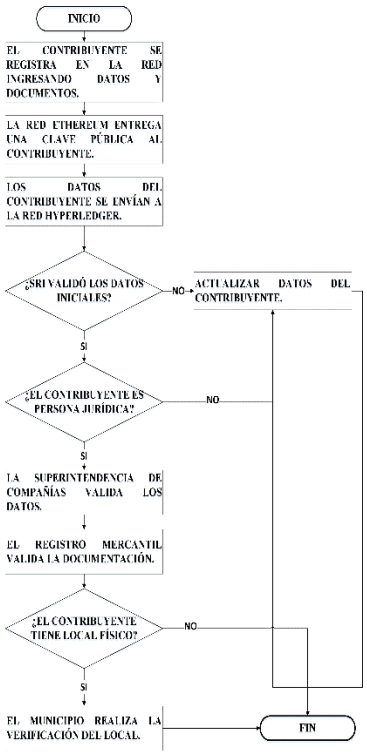


Fig. 3. Creación de contribuyente.

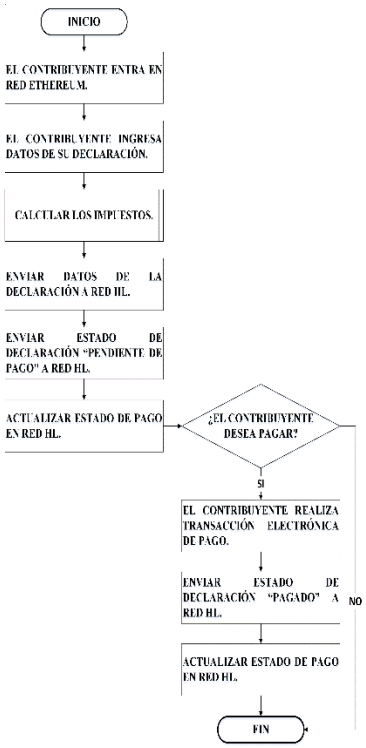


Fig. 4. Declaración de impuestos.

3.3 Evaluación del rendimiento de la arquitectura híbrida a través de una simulación.

El fundamento matemático para medir el rendimiento teórico de la arquitectura hibrida se expresa en la formula (1):

$$R = \frac{(\text{RTotal} - \text{RSuccess})/\text{RSuccess}}{\sqrt{\text{Users} + \text{Interac}}} \qquad (1)$$

Aquí:

- Rtotal es la cantidad de registros enviados para almacenamiento
- Rsuccess es la cantidad de registros almacenados en la arquitectura
- Users es la cantidad de usuarios que utilizan el sistema
- Interac es la cantidad de interacciones en las aplicaciones

Para el ensayo con las variables se determinaron valores aleatorios; para los registros enviados se determinaron valores entre 500 a 1500; para los registros almacenados se determinaron valores entre 100 a 1000; para los usuarios que utilizan el sistema se determinaron valores entre 100 a 1000; para las interacciones en las aplicaciones, los valores van desde 500 a 1500.

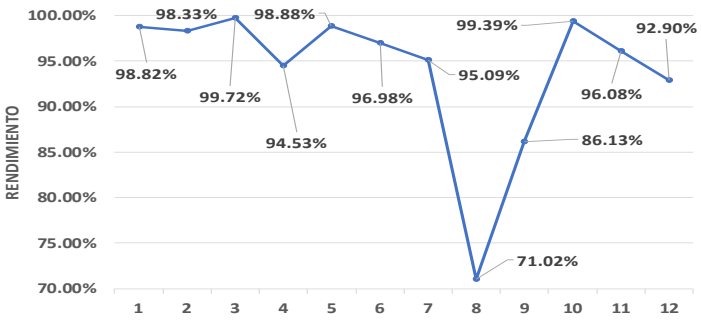


Fig. 5. Rendimiento de la arquitectura.

La Fig. 5 muestra los porcentajes de eficiencia del modelo propuesto en una simulación de doce escenarios para aplicar la fórmula; en el primer escenario ingresaron 312 usuarios con una interacción de las aplicaciones 733, el total de las transacciones fue 503 con 364 transacciones exitosas y con una tasa de falla 1.18%, es decir el rendimiento fue 98.82%; en el sexto escenario ingresaron 483 usuarios con una interacción de las aplicaciones 1431, el total de las transacciones fue 791 con 341 transacciones exitosas y con una tasa de falla 3.02%, es decir el rendimiento fue 96.98%; en el octavo escenario ingresaron 622 usuarios con una interacción de las aplicaciones 526, el total de las transacciones fue 1244 con 115 transacciones exitosas y con una tasa de falla 28.98%, es decir el menor rendimiento fue 71.02%; se deduce que el rendimiento está en función de la cantidad de transacciones que se almacenaron versus la cantidad de transacciones que se enviaron a la red híbrida.

4 Discusión

Relación de los resultados: Se revisaron los participantes públicos y privados que entran en el esquema de seguridad para formar la cadena de datos; estos participantes están relacionados y actúan sobre la arquitectura híbrida, ejecutan las funciones del Smart Contract y actúan de acuerdo al orden de los algoritmos presentados; la fórmula propuesta para evaluar el rendimiento teórico de la arquitectura híbrida está en base a transacciones, usuarios y aplicaciones, a través de una simulación en doce escenarios.

Nuestra investigación concuerda: con [7] en el pago de impuestos; con [9] por diseño de plataforma informática para el pago de impuestos; con [10] por el pago de impuestos; con [9] por el diseño del modelo en 3 capas, con [11] por una arquitectura de 3 capas; con [12] por el diseño de una arquitectura de 4 capas; con [13] por el diseño una red BK en una organización pública; con [14] por el diseño de una red BK mixta para el sistema de datos públicos, aquí la parte pública está en Ethereum para los ciudadanos, la parte privada está en Hyperledger para las organizaciones públicas.

Excepciones: no se considera tiempos, ni personal, ni costos para el diseño, desarrollo o implementación para la arquitectura propuesta; el software que se nombró puede variar de acuerdo a los proveedores o nuevas versiones; las velocidades o eficiencias de una arquitectura depende de las redes físicas, equipos de computación y sistemas operativos; en la red pública sólo tienen acceso los contribuyentes, no está considerado el acceso a todo ciudadano que es un interesado en conocer los impuestos declarados a la autoridad tributaria.

Como una aplicación práctica: Propusimos utilizar la tecnología BK en la declaración de impuestos con una plataforma privada para el control y una plataforma pública para la declaración; la implementación es posible en un sólo proceso para observación del impacto en la organización pública y en los ciudadanos.

Aplicar la tecnología BK al área de impuestos tiene desafíos como: la distribución de datos al mismo tiempo de conservar la privacidad y el procesamiento de estos datos; los reclamos de los contribuyentes, interacción entre los interesados, autenticidad de otros tipos de interesados, estándares de presentación de datos y escalabilidad de los datos.

5 Conclusiones

Se concluyó que el modelo propuesto formado por los participantes, arquitectura híbrida en Hyperledger/Ethereum, funciones y los algoritmos, brindan un mayor nivel de seguridad a la información que se origina en los contribuyentes y es procesada por la entidad estatal a través de la tecnología blockchain que mantiene los datos con transparencia, privacidad y seguridad; en las simulaciones teóricas del modelo el menor rendimiento fue 71.02% y máximo rendimiento fue 99.39%; se dedujo que el rendimiento está en función de la cantidad de transacciones que se almacenaron versus la cantidad de transacciones que se enviaron a la red híbrida.

El primer resultado propuso los participantes básicos para el modelo propuesto; el segundo resultado propuso la arquitectura híbrida formada en Hyperledger para acceso privado y en Ethereum para acceso público, además de lista de funciones con los responsables, y algoritmos para el funcionamiento de la arquitectura; el tercer resultado demostró la eficiencia del modelo propuesto.

Blockchain es una tecnología disruptiva que se aplica en muchas áreas, especialmente para seguimiento, auditoría, datos inmutables y consenso; por sus características es una buena alternativa para aplicar a entidades estatales o de gobierno.

Acknowledgment

Thanks to Universidad Politécnica Salesiana del Ecuador (Sede Guayaquil).

References

1. Fatz, F., Hake, P., Fettke, P.: Towards Tax Compliance by Design: A Decentralized Validation of Tax Processes Using Blockchain Technology. 2019 IEEE 21st Conf. Bus. Informatics. 1, 559–568 (2019). https://doi.org/10.1109/CBI.2019.00071

2. Zhang, Y., Xu, X., Liu, A., Lu, Q., Xu, L., Tao, F.: Blockchain-Based Trust Mechanism for IoT-Based Smart Manufacturing System. IEEE Trans. Comput. Soc. Syst. 6, 1386–1394 (2019). https://doi.org/10.1109/TCSS.2019.2918467

3. Lund, E.K., Nowostawski, M., Satybaldy, A., Aeinehchi, N.: Privacy-preserving tax-case processing. 2019 17th Int. Conf. Privacy, Secur. Trust. 1–10 (2019). https://doi.org/10.1109/PST47121.2019.8949072

4. Wibowo, S., Sandikapura, T.: Improving Data Security, Interoperability, and Veracity using Blockchain for One Data Governance, Case Study of Local Tax Big Data. 2019 Int. Conf. ICT Smart Soc. 1–6 (2019). https://doi.org/10.1109/ICISS48059.2019.8969805

5. Gupta, N., Das, M.L., Nandi, S.: LandLedger: Blockchain-powered Land Property Administration System. 2019 IEEE Int. Conf. Adv. Networks Telecommun. Syst. 2019-Decem, 1–6 (2019). https://doi.org/10.1109/ANTS47819.2019.9118125

6. Malik, G., Parasrampuria, K., Reddy, S.P., Shah, S.: Blockchain Based Identity Verification Model. 2019 Int. Conf. Vis. Towar. Emerg. Trends Commun. Netw. 1–6 (2019). https://doi.org/10.1109/ViTECoN.2019.8899569

7. Zinca, D., Negrean, V.-A.: Development of a Road Tax Payment Application using the Ethereum Platform. 2018 Int. Symp. Electron. Telecommun. 1–4 (2018). https://doi.org/10.1109/ISETC.2018.8583975

8. Ecuador: Servicio de Rentas Internas, https://www.sri.gob.ec/web/guest/home

9. NGUYEN, V.-C., PHAM, H.-L., TRAN, T.-H., HUYNH, H.-T., NAKASHIMA, Y.: Digitizing Invoice and Managing VAT Payment Using Blockchain Smart Contract. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). pp. 74–77. IEEE (2019)

10. Lu, Z., Wan, X., Yang, J., Wu, J., Zhang, C., Hung, P.C.K., Huang, S.-C.: Bis: A Novel Blockchain Based Bank-Tax Interaction System in Smart City. 2019 IEEE Intl Conf Dependable, Auton. Secur. Comput. Intl Conf Pervasive Intell. Comput. Intl Conf Cloud Big Data Comput. Intl Conf Cyber Sci. Technol. Congr. 1008–1014 (2019). https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00183

11. Chiliveri, S., Grandhi, J., Uttam Patil, M., P.R., L.E., Ethirajan, M.: ProveDoc: A Blockchain Based Proof of Existence with Proof of Storage. 2019 Int. Conf. Inf. Technol. 239–244 (2019). https://doi.org/10.1109/ICIT48102.2019.00049

12. Nugraha, I.G.B.B., Bandung, Y., Zaky, A.: Official Document Management for Government Service in Indonesia using Smart Contract. 2019 IEEE Int. Smart Cities Conf. 390–395 (2019). https://doi.org/10.1109/ISC246665.2019.9071643

13. Toapanta, S.M.T., Quimi, F.G.M., Espinoza, M.G.T., Gallegos, L.E.M.: Proposal of a Model to Apply Hyperledger in Digital Identity Solutions in a Public Organization of Ecuador. 2019 Third World Conf. Smart Trends Syst. Secur. Sustain. 21–28 (2019). https://doi.org/10.1109/WorldS4.2019.8903981

14. Toapanta Toapanta, S.M., Mafla Gallegos, L.E., Ordonez Baldeon, P., Trivino Trivino, F.D.: Blockchain Analysis Applied to a Process for the National Public Data System for Ecuador. 2020 3rd Int. Conf. Inf. Comput. Technol. 258–265 (2020). https://doi.org/10.1109/ICICT50521.2020.00046

15. Aleksieva, V., Valchanov, H., Huliyan, A.: Implementation of smart-contract, based on hyperledger fabric blockchain. 2020 21st Int. Symp. Electr. Appar. Technol. SIELA 2020 - Proc. 1–4 (2020). https://doi.org/10.1109/SIELA49118.2020.9167043

16. Oktian, Y.E., Witanto, E.N., Kumi, S., Lee, S.-G.: BlockSubPay - A Blockchain Framework for Subscription-Based Payment in Cloud Service. 2019 21st Int. Conf. Adv. Commun. Technol. 2019-Febru, 153–158 (2019). https://doi.org/10.23919/ICACT.2019.8702008

17. Deshmukh, P., Kalwaghe, S., Appa, A., Pawar, A.: Decentralised Freelancing using Ethereum Blockchain. 2020 Int. Conf. Commun. Signal Process. 881–883 (2020). https://doi.org/10.1109/ICCSP48568.2020.9182127

18. Tas, R., Tanriover, O.O.: Building A Decentralized Application on the Ethereum Blockchain. 2019 3rd Int. Symp. Multidiscip. Stud. Innov. Technol. 1–4 (2019). https://doi.org/10.1109/ISMSIT.2019.8932806

19. Manzoor, A., Hu, Y., Liyanage, M., Ekparinya, P., Thilakarathna, K., Jourjon, G., Seneviratne, A., Kanhere, S., Ylianttila, M.E.: Demo: A Delay-Tolerant Payment Scheme on the Ethereum Blockchain. 2018 IEEE 19th Int. Symp. “A World Wireless, Mob. Multimed. Networks.” 14–16 (2018). https://doi.org/10.1109/WoWMoM.2018.8449794

20. Harer, F., Fill, H.-G.: Decentralized Attestation of Conceptual Models Using the Ethereum Blockchain. 2019 IEEE 21st Conf. Bus. Informatics. 104–113 (2019). https://doi.org/10.1109/CBI.2019.00019

21. Nemade, A.E., Kadam, S.S., Choudhary, R.N., Fegade, S.S., Agarwal, K.: Blockchain Technology used in Taxation. 2019 Int. Conf. Vis. Towar. Emerg. Trends Commun. Netw. 1–4 (2019). https://doi.org/10.1109/ViTECoN.2019.8899652

22. Toapanta Toapanta, S.M., Prado Quintana, T.F., Maciel Arellano, M.R., Mafla Gallegos, L.E.: Hyperledger Technology in Public Organizations in Ecuador. 2020 3rd Int. Conf. Inf. Comput. Technol. 294–301 (2020). https://doi.org/10.1109/ICICT50521.2020.00052