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 BLOCKCHAIN PARA AUMENTAR LA INTEGRIDAD DE INFORMACIÓN MEDIANTE TECNOLOGÍA HYPERLEDGER PARA EL SEGURO SOCIAL”

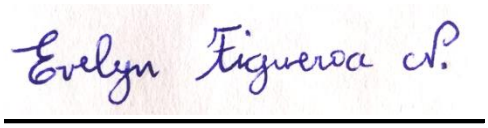
AUTOR:
FIGUEROA NAVARRO EVELYN TAMARA

TUTOR:
MSG. TANDAZO ESPINOZA MÁXIMO GIOVANI

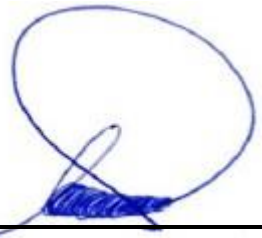
JUNIO 2021
GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **FIGUEROA NAVARRO EVELYN TAMARA,** declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.



Nombre: Evelyn Tamara Figueroa Navarro
CI. 0953001708



Nombre: Máximo Giovani Tandazo Espinoza
CI. 0916028921

MODELO DE BLOCKCHAIN PARA AUMENTAR LA INTEGRIDAD DE INFORMACIÓN MEDIANTE TECNOLOGÍA HYPERLEDGER PARA EL SEGURO SOCIAL

Máximo Giovani Tandazo Espinoza[1[0000-0002-8844-9384]] and Evelyn Tamara Figueroa Navarro[1[0000-0003-4982-7677]]

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

Abstract. Different proposals were analyzed in first level bibliographic references on hyperledger. The problem is maintaining integrity, privacy, traceability and free of information changes, and having a scalable platform for Social Security. The objective is to design a Blockchain model to increase information integrity using Hyperledger Technology for Social Security. The methodology applied to the study of the subject presented will be with a qualitative approach that will allow us to perform an analysis of the models in Hyperledger that manage or manage information; the method of observation and deduction. The results are Study of the model and use of Hyperledger technology for information storage and security, Hyperledger Conceptualizing a model for information security and social security data management using Hyperledger technology, and assessing the efficiency of the proposed model using theoretical simulations. It was concluded that hyperledger technology gives a higher level of security to information with its privacy and immutability properties that are embodied in the proposed model; in theoretical simulation the minimum efficiency is 99.81% and the maximum efficiency is 100%, it follows that the lower the number of records in the ledger the higher the efficiency, the number of attentions or transactions do not influence the efficiency.

Keywords: Blockchain, Hyperledger, Integrity information, Distributed Architecture.

1 Introducción

En la actualidad la tecnología Blockchain ha sido muy revolucionaria para la comercialización digital, la integridad con la información que se manejan con el uso del sistema, la encriptación y los modelos de autenticidad que proporcionan los contratos

inteligentes, ha probado ser una tecnología que brinda seguridad en las transacciones y transferencias de información [1].

Blockchain es una cadena o lista de bloques que están cifrados y contiene transacciones encapsuladas y firmadas digitalmente, son verificadas por los participantes de la red, cada usuario tiene una réplica del ledger y funciones, además es una red peer-to-peer; los participantes generan transacciones validas con claves públicas y privadas; cada participante genera la transacción con firma digital y clave privada; la cadena de bloques se mantiene inalterable o inmutable, la criptografía garantiza no leer o tener la clave privada de la firma digital[2]. La cadena de bloques se divide en público blockchains que tiene la plataforma Ethereum y blockchains privados que tiene la plataforma Hyperledger, esta última cuenta con servicio de membresía para entidades/usuarios autorizados[3].

El Blockchain privado es una opción por la confiablidad de sus nodos, tiene acceso rápido a la cadena de datos, las transacciones son más económicas en tiempo, existe control a nivel de privacidad[4]; en [5] está un análisis y comparación entre plataformas blockchain, en base a esto se elige Hyperledger Fabric que es privado para el desarrollo de Smart Contracts.

Hyperledger Fabric es un entorno distribuido y privado, para ambientes de confianzas entre los pares o empresas que forman un consorcio; es más sencilla para formar una red blockchain y ajustarlo al modelo de negocio de las empresas; es de código abierto, factible a mejoras y adaptable a necesidades[4].

El Smart Contracts son scripts/líneas ejecutables almacenadas en el blockchain, todos los participantes/pares ejecutan el script en la red para cumplir los procesos del contrato[2].

El manejo de la información y el sistema informático del Seguro Social provoca una saturación en el sistema de acuerdo con la demanda de transacciones realizadas a última hora por parte de los usuarios al realizar los trámites, la falta del control en la entrega de credenciales personales produjera perdidas en la información e infiltración de terceros al sistema de almacenamiento del Seguro Social [6].

La conceptualización de un modelo de Blockchain propone mejorar la administración de la información en el sistema del Seguro Social como la integridad y seguridad mediante la inmutabilidad de los datos.

La tecnología Blockchain nos permite mejorar la confiabilidad de los datos que se ingresen en el sistema del Seguro Social, de acuerdo con el modelo de Hyperledger lograremos mejorar la confidencialidad, flexibilidad e integridad de la información con el modelo de registro compartido, encapsulado y con la implementación de la tecnología de los contratos inteligentes [7].

El problema es mantener la integridad, privacidad, trazabilidad y libre de cambios a la información, y tener una plataforma escalable para el Seguro Social.

La pregunta de investigación es: ¿Por qué es necesario un modelo de blockchain para aumentar la integridad de la información mediante tecnología Hyperledger para el Seguro Social?

Para mantener un modelo de administración de la información en el sistema del Seguro Social con la finalidad de brindar confiabilidad en el uso de la información y

respaldo de los datos generados por un administrador de proyecto de la seguridad de la información y brindar a los usuarios respuesta optima en los sistemas de la entidad.

Implementar el modelo de Blockchain para el sistema del Seguro Social permitirá a la información ser tratada en los nodos en los que se almacenan, antes de ser manejadas, los datos almacenados podrán ser respaldados y puestos a pruebas mediante simulaciones que lograrán alzar los niveles de confianza con los usuarios que utilizan el sistema.

El objetivo es diseñar un modelo de Blockchain para aumentar la integridad de información mediante tecnología Hyperledger para el Seguro Social.

La metodología aplicada al estudio del tema expuesto será con enfoque cualitativo que nos permitirá realizar un análisis de los modelos en Hyperledger que manejan o administran información; el método de la observación y la deducción.

2 Revisión de la literatura

Se realiza un análisis de otros trabajos para explicar el modelo de cadena de bloques Hyperledger como un modelo de administración y seguridad en la integridad de los datos del sistema del Seguro Social.

Los sistemas de comercialización electrónica de [1] utilizaron un modelo de cadena de bloques con tecnología Hyperledger para un sistema de autenticación de credenciales de usuarios que les permitieron manejar las transacciones de punto a punto con la confidencialidad y mejora de administración de datos en el trayecto del envió o del intercambio de información. Para mejorar el modelo de transferencias de información y el desarrollo del sistema de almacenamiento de acuerdo con el estudio planteado en este trabajo a través de la tecnología Hyperledger [2]. En las organizaciones de manejo de información económica o de datos sensibles, en los negocios de seguros proponen un modelo de seguridad en Hyperledger para mejorar los procesos de transacciones y validación de pagos mediante contratos inteligentes [4]. La ley del Seguro Social propone que toda la información que se almacena de las empresas que aseguran a sus empleadores no se administran de manera optimas y la confiabilidad de los datos no brinden una respuesta ágil a los usuarios que hacen uso de los servicios del sistema de la entidad [6]. Para salvaguardar el registro y la ejecución de los servicios o transacciones de las empresas se propone un modelo de cadena de bloque basada en Hyperledger, lograron una garantía la sistema de traspaso de información autónoma [7]. El modelo de Blockchain al utilizar Hyperledger Fabric para la autenticación de pares mediante tokens que generan las credenciales que son proporcionadas para el uso del sistema y que sea confiable para los usuarios [3]. En una red de datos utilizada para intercambiar información de carácter comercial se necesitan un modelo de intercambio seguro, los autores proponen Hyperledger para servir como una seguridad de intercambio compartido para realizar transacciones comerciales [8]. Los contratos inteligentes que se proponen en [9] permiten mejorar el modelo de transferencias y administración de la información que se maneja en las instituciones financieras. Los autores proponen un modelo en Hyperledger para mejorar los índices de rendimiento en las transacciones exitosas, el tiempo de respuesta y la escalabilidad en la información tratada por los administradores de base de datos en las empresas [10]. Para el uso de la tecnología

Blockchain se analizan en [11] los modelos que Hyperledger que son Fabric, Sawtooth y Caliper, con el estudio de las tecnologías se busca comparar y elegir que tecnología servirá para el trabajo expuesto, cada modelo se basa en un campo en específico, para el sistema de autenticación e integridad de la información, Hyperledger Fabric cumple los requisitos de acuerdo al análisis empleado por los autores. Para el procesamiento de datos en el sector público y privado en [12], con Hyperledger garantizan un procesamiento de información con implementación de autenticación y un proceso simultaneo entre pares con la finalidad de aumentar la disponibilidad en el sistema. En [13] se aplicó la tecnología Blockchain para mejorar la calidad de relación en la confianza en los sectores empresariales, instituciones financieras, entre otros. Para mejorar la confiabilidad de los registros en el sistema de almacenamiento de un establecimiento médico los autores proponen un sistema de almacenamiento seguro con el uso de Hyperledger que les permite manejar la interacción entre un grupo de participantes [14]. En la seguridad de los datos, los autores utilizan Hyperledger para el almacenamiento y uso de la información de datos privados con una variación de un sistema protegido mientras se realiza una transacción [15]. Para la protección de las transferencia de información y seguridad en el sistema de almacenamiento, los autores proponen un sistema con tecnología Hyperledger para la verificación de transacciones, protección de los datos y del sistema de acuerdo a la autenticidad con pares para generar estabilidad al tiempo de respuesta y garantizar una transacción exitosa para los usuarios [16].

3 Métodos

La metodología aplicada al estudio del tema expuesto será con enfoque cualitativo que nos permitirá realizar un análisis de los modelos en Hyperledger que manejan o administran información; el método de la observación y la deducción.

Alcance de esta investigación

- Comparar los modelos en hyperledger obtenidos desde las referencias, describir características como proceso, método y eficiencia
- Confirmar los participantes para la red blockchain
- Nombrar las funciones que tendrá el Smart Contract
- Nombrar los participantes del consorcio
- Proponer una arquitectura o modelo conceptual basada en Hyperledger
- Describir cada capa o nivel de la arquitectura con sus funciones y sus elementos
- Evaluar el modelo por medio de simulaciones en hoja electrónica

Participantes del modelo en hyperledger

- Seguro Social y Centros de Salud del Seguro Social

Integrantes del Consorcio

- Seguro Social y Centros de Salud del Seguro Social

Participantes excluidos

- Empleador, Bancos de terceros, Afiliados, banco del seguro social, centros de salud de terceros

Estados de un afiliado

- Activo, Inactivo, Cesante

4 Resultados

En esta fase de obtuvieron los siguientes resultados:

- Estudio del modelo y el uso de la tecnología Hyperledger para el almacenamiento y seguridad de la información.
- Conceptualización de un modelo para la seguridad de la información y administración de los datos del Seguro Social mediante tecnología Hyperledger.
- Evaluación de la eficiencia del modelo propuesto mediante simulaciones teóricas.

4.1 Estudio del modelo y el uso de la tecnología Hyperledger para el almacenamiento y seguridad de la información

Se da a conocer algunos modelos que utilizaron hyperledger para gestionar información; en Tabla 1 se encuentran las propuestas, los objetivos y como los autores de las referencias midieron cada modelo; no todos realizan alguna verificación cuantitativa.

Table 1. Modelos en hyperledger.

Ref.	Propuesta	Objetivo	Medición del modelo
[1]	Sistema de autenticación de credenciales para usuarios y gestión de transacciones	Preservar la privacidad	1000 estados en 500 milisegundos
[2]	Transferencias de información y el desarrollo del sistema de almacenamiento	Eficiencia del sistema	112 milisegundos por transacción
[3]	Códigos de autenticación para los usuarios que utilizan el sistema	Prevenir vulnerabilidades	Pruebas, No hay Métrica
[4]	Procesos de transacciones y validación de pagos mediante contratos inteligentes	Seguridad de transacciones y velocidad de pagos	Pruebas, No hay Métrica
[7]	Servicios bancarios controlados por tiempo sobre una cadena de bloques	Rastreo de los servicios	No hay métrica
[8]	Intercambio de transacciones comerciales con flujos de control	Seguridad de intercambio compartido	No hay métrica
[9]	Datos correctos en guardado y almacenamiento y operabilidad de la red	Rastreo de la información	Pruebas, No hay Métrica
[10]	Evaluación de rendimiento, latencia y escalabilidad	Índices de rendimiento en transacciones	Entre 0.01 y 0.16 segundos por 100mil transacciones
[11]	Comparación de versiones de hyperledger	Pruebas de rendimiento	900 transacciones por segundo
[12]	Arquitectura de red inteligente	Procesamiento de información con autenticación y disponibilidad	0.1 unidad de tiempo
[13]	Sistema de servicios de salud	Registro de transacciones accesibles y controlados	Pruebas, No hay Métrica
[14]	Arquitectura para gestionar registros médicos electrónicos	Garantizar la seguridad y la privacidad de los datos del paciente.	No hay Métrica

[15]	Sistema de licitación de activos entre vendedores y postores	Mantener privacidad de datos	0.3s por transacción
[16]	Sistema de transporte inteligente	Estabilidad y confianza del servicio	Latencia de comunicación 0.1s para vehículos

4.2 Conceptualización de un modelo para la seguridad de la información y administración de los datos del Seguro Social mediante tecnología Hyperledger.

El modelo está formado por una arquitectura, lista de funciones del Smart Contract que se describen a continuación:

Arquitectura basada en tecnología hyperledger: El administrador es un nodo que inicia el Ordering Service (OS) y realiza la configuración de la red, este tiene los derechos de administrador de la red del Seguro Social, además tiene su propio Certificado de Autenticación (CA) que lo utiliza para entregar identidades a los administradores y nodos de la red; el administrador adiciona al Seguro Social como administrador en la Configuración de Red (CR); el Seguro Social tiene su CA; el administrador define el Consorcio formado por las organizaciones Seguro Social y el Centro de Salud, este consorcio es almacenado en la CR; se adicionan los CA del Seguro Social y del Centro de Salud a las organizaciones; el Canal de Comunicación (CC) está formado por las organizaciones definidas en el Consorcio, el CC es administrador por las dos organizaciones y tienen igual derecho, el Administrador no tiene derechos sobre el CC; el Seguro Social crea su Nodo-Seguro-Social para unirlo al canal, el Nodo es físicamente un host con una copia del Ledger y del Smart Contract, ahora el nodo y el OS se conectan a través del canal, el Seguro Social adiciona una aplicación-cliente para consumir los servicios de la red blockchain; el Centro de Salud también crea su Nodo-CentroSalud que tiene una copia del Ledger y del Smart Contract, este nodo y la aplicación-cliente del Centro de Salud se conectan al canal a través del CA; las aplicaciones clientes invocan al Smart Contract que está conectado al CC a través de los nodos.

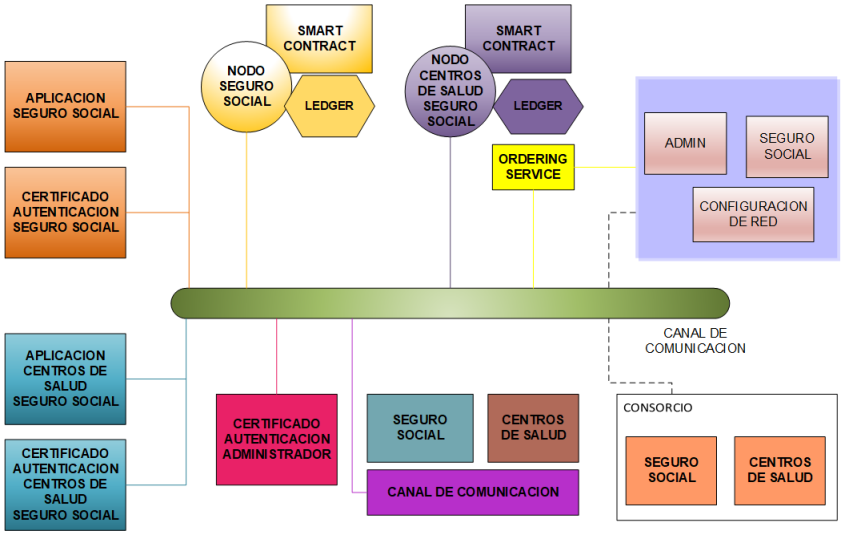


Fig. 1. Arquitectura de seguridad basada en hyperledger.

Activos (Assets): Los activos de información son los recursos que se utiliza en el negocio, y son valores claves de la red corporativa.

- Afiliado: contiene los datos básicos del afiliado o empleado, como: cédula, apellidos, nombres, dirección, teléfono, correo electrónico, fecha de nacimiento, fecha de defunción, estado del empleado.
- Patrono: contiene los datos básicos del empleador, como: identificación, nombres, dirección, teléfono, correo electrónico, fecha de inicio.
- Afiliaciones: contiene las relaciones del afiliado con los patronos para las cuales laboró, entre los datos están: identificación del patrono, identificación del afiliado, fecha de ingreso, fecha de salida, cargo del afiliado.
- Historial de Aportaciones: contiene las aportaciones del afiliado realizadas por cada patrono, entre los datos están: identificación del patrono, tipo de aportación, fecha de aportación, valor de aportación, disponibilidad de aportación.
- Centros de Salud: contiene los datos básicos de cada centro como: identificación, nombre, dirección, ciudad, provincia, teléfonos.
- Atenciones de Salud: contiene los registros de cada atención medica del afiliado, entre los datos están: identificación de la cita médica, fecha de cita, hora, nombre del médico, nombre de especialidad, identificación del centro, peso, estatura, presión, descripción del problema, prescripción médica, receta, tiempo de atención, próxima cita posible.

Funciones del Smart Contract: Las funciones generan cada transacción con timestamp e identificación de la transacción.

- Crear afiliado: genera un nuevo afiliado en el seguro social, responsable seguro social

- Actualiza afiliado: actualiza el estado del afiliado, responsable S.S.
- Crear patrono: genera un nuevo empleador en el seguro social, responsable S.S.
- Crear afiliaciones: genera las afiliaciones entre afiliado y patrono, responsable S.S.
- Crear historial de Aportaciones: genera cada aportación del afiliado, responsable S.S.
- Crear centros de Salud: genera un nuevo centro de salud, responsable S.S.
- Crear atenciones de Salud: genera un registro para atención del afiliado en un centro de salud, responsable centro de salud.
- Actualizar atenciones de Salud: actualiza la información después de la atención medica al afiliado, responsable centro de salud.

4.3 Evaluación de la eficiencia del modelo propuesto mediante simulaciones teóricas.

En base a la cantidad de transacciones que tendría la red blockchain, se propone un fundamento matemático para verificar la eficiencia en la integridad de la información que se expresa en la formula (1):

$$Eficiencia = \left(\frac{\text{Atenciones} + \sqrt{Registros}}{\text{Transacciones}}\right)^{\frac{1}{Transacciones}} \quad (1)$$

Aquí:

- Atenciones es la cantidad de atenciones médicas que se presentan en el sistema.
- Registros es la cantidad de registros almacenados en todo el ledger.
- Transacciones es la cantidad de transacciones diarias generadas por los pacientes que se lograron atender.

Para simular la eficiencia del modelo en hoja electrónica, las variables se generaron con valores aleatorios; la cantidad de atenciones se obtuvo valores entre 100 a 500 en un instante de tiempo; para la cantidad de registros almacenados en la cadena de bloques se obtuvo valores entre 1000 a 5000; para la cantidad de transacciones se obtuvo valores entre de 500 a 1000. La Fig. 2 se muestra la simulación de la formula en diez escenarios; el eje X principal es la cantidad de transacciones, el eje X secundario es el porcentaje para la eficiencia, el eje Y es cada escenario; para el primer escenario se obtuvieron 332 atenciones, 2138 registros, 699 transacciones con una eficiencia de 99.91%; para el sexto escenario se obtuvieron 329 atenciones, 4277 registros, 527 transacciones con una eficiencia de 99.95%; el mejor escenario es el tercero con 475 atenciones, 1109 registros, 521 transacciones con una eficiencia de 100%; el mínimo porcentaje es 99.81% de eficiencia; se deduce que entre menor cantidad de registros en el ledger es más alta la eficiencia, la cantidad de atenciones o transacciones no influyen en la eficiencia.

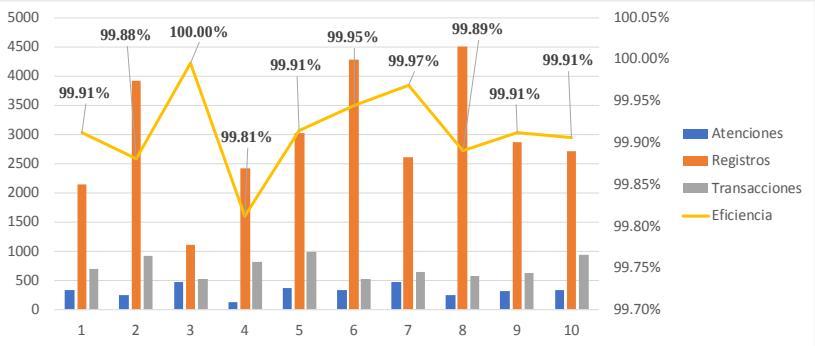


Fig. 2. Eficiencia del modelo.

5 Discusión

Relación de los resultados: en el primer resultado se analizaron modelos donde se utilizó hyperledger en casos de almacenamiento y seguridad; en base a las lecturas se conceptualizó un modelo para la seguridad de la información basado en tecnología hyperledger que contiene una arquitectura, activos de información y funciones; el modelo fue evaluado en su eficiencia a través simulaciones teóricas en hoja electrónica.

Esta investigación concuerda con [8] en la aplicación de seguridad; concuerda con [2] en la medición de eficiencia del modelo, concuerda con [4] en la aplicación de seguridad a los datos, concuerda con [13] y [14] en la aplicación de hyperledger a servicios de salud.

Excepciones: Este documento solo presenta el diseño del modelo propuesto; no se diseñaron interfaces, no se nombran herramientas para implementación, kit de desarrollo, sistemas operativos, cronogramas de desarrollo, ni costos monetarios; existen varios framework de hyperledger es necesario otra investigación para determinar que versión utilizar.

No es novedad la estructura de datos propuesta para el seguro social, la novedad es la utilización de tecnología hyperledger y sus definiciones básicas para aplicar en un servicio específico del seguro social; este documento solo se enfoca en el diseño de la red presentado en una arquitectura, funciones y eficiencia teórica.

La consecuencia teórica de esta propuesta puede servir para planes de implementación a través de software, mejoras al modelo a la arquitectura, optimización de las funciones y mejoras a los activos de datos.

6 Conclusiones

Se concluyó que la tecnología hyperledger da un mayor nivel de seguridad a la información con sus propiedades de privacidad e inmutabilidad que están plasmadas en el modelo propuesto; en la simulación teórica la eficiencia mínima es 99.81% y la eficiencia máxima es 100%, se deduce que entre menor cantidad de registros en el ledger

es más alta la eficiencia, la cantidad de atenciones o transacciones no influyen en la eficiencia.

Los objetivos específicos del anteproyecto fueron alcanzados a través de los resultados propuestos, otra manera de mantener la integridad de la información es a través del cifrado que mantiene blockchain en el ledger, y los certificados de autenticación que se entregan a los participantes.

Hyperledger es una tecnología que está en proceso de maduración, no toda tecnología se puede aplicar en toda área, su ledger distribuido y compartido mantiene la integridad de la información en su cadena de bloques.

Como trabajo futuro se propone una arquitectura de datos seguros para las aportaciones de los afiliados al seguro social mediante tecnología hyperledger.

Acknowledgment

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

References

1. Androulaki, E., De Caro, A., Neugschwandtner, M., Sorniotti, A.: Endorsement in Hyperledger Fabric. In: 2019 IEEE International Conference on Blockchain (Blockchain). pp. 510–519. IEEE (2019)
2. Mokhtar, A., Murphy, N., Bruton, J.: Blockchain-based multi-robot path planning. In: IEEE 5th World Forum on Internet of Things, WF-IoT 2019 - Conference Proceedings. pp. 584–589. IEEE (2019)
3. Park, W., Hwang, D., Kim, K.: A TOTP-Based Two Factor Authentication Scheme for Hyperledger Fabric Blockchain. In: 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN). pp. 817–819. IEEE (2018)
4. Aleksieva, V., Valchanov, H., Huliyan, A.: Implementation of Smart Contracts based on Hyperledger Fabric Blockchain for the Purpose of Insurance Services. In: 2020 International Conference on Biomedical Innovations and Applications (BIA). pp. 113–116. IEEE (2020)
5. Rashid, A., Siddique, M.J.: Smart Contracts Integration between Blockchain and Internet of Things: Opportunities and Challenges. In: 2019 2nd International Conference on Advancements in Computational Sciences (ICACS). pp. 1–9. IEEE (2019)
6. Porras, A.V.: La seguridad social en Ecuador: un necesario cambio de paradigmas. Foro 24, II Semest. 2015. 89–116 (2015)
7. Lee, Y.T., Lin, J.J., Hsu, J.Y.J., Wu, J.L.: A Time Bank System Design on the Basis of Hyperledger Fabric Framework. IEEE Int. Conf. Blockchain Cryptocurrency, ICBC 2020. 1–16 (2020). https://doi.org/10.1109/ICBC48266.2020.9169476
8. Chua, P.H.T., Li, Y., He, W.: Adopting Hyperledger Fabric Blockchain for EPCglobal Network. In: 2019 IEEE International Conference on RFID (RFID). pp. 1–8. IEEE (2019)
9. Aleksieva, V., Valchanov, H., Huliyan, A.: Implementation of smart-contract, based on hyperledger fabric blockchain. In: 2020 21st International Symposium on Electrical

Apparatus and Technologies, SIELA 2020 - Proceedings. pp. 1–4. IEEE (2020)
10. Kuzlu, M., Pipattanasomporn, M., Gurses, L., Rahman, S.: Performance analysis of a hyperledger fabric blockchain framework: Throughput, latency and scalability. Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019. 536–540 (2019). https://doi.org/10.1109/Blockchain.2019.00003
11. Ampel, B., Patton, M., Chen, H.: Performance modeling of hyperledger sawtooth blockchain. 2019 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2019. 59–61 (2019). https://doi.org/10.1109/ISI.2019.8823238
12. Kim, Y., Kim, K.H., Kim, J.H.: Power Trading Blockchain using Hyperledger Fabric. Int. Conf. Inf. Netw. 2020-Janua, 821–824 (2020). https://doi.org/10.1109/ICOIN48656.2020.9016428
13. Wutthikarn, R., Hui, Y.G.: Prototype of blockchain in dental care service application based on hyperledger composer in hyperledger fabric framework. 2018 22nd Int. Comput. Sci. Eng. Conf. ICSEC 2018. 2018–2021 (2018). https://doi.org/10.1109/ICSEC.2018.8712639
14. Alshalali, T., Mbale, K., Josyula, D.: Security and privacy of electronic health records sharing using hyperledger fabric. Proc. - 2018 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2018. 760–763 (2018). https://doi.org/10.1109/CSCI46756.2018.00152
15. Benhamouda, F., Halevi, S., Halevi, T.: Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation. In: 2018 IEEE International Conference on Cloud Engineering (IC2E). pp. 357–363. IEEE (2018)
16. Lee, Y., Jeong, S., Masood, A., Park, L., Dao, N.-N., Cho, S.: Trustful Resource Management for Service Allocation in Fog-Enabled Intelligent Transportation Systems. IEEE Access. 8, 147313–147322 (2020). https://doi.org/10.1109/ACCESS.2020.3015550