








Modelo de arquitectura de seguridad de datos aplicando Blockchain en los procesos de admisión de una universidad Peruana

Data security architecture model applying Blockchain in the admission processes of a Peruvian university

Roxana Janet Quiroz Valenzuela, Maestra¹  Félix José Colina Ysea, Doctor²  Cristofher Zúñiga Vargas, Doctor³ 
Denis Christian Ovalle Paulino, Doctor⁴  Jean Luis Arana Alencastre, Maestro⁵  Oscar Gutiérrez Baracco,
Estudiante⁶  y Omar Peralta Palomino, Estudiante⁷ 
Universidad Tecnológica del Perú, Perú, c02287@utp.edu.pe, c19271@utp.edu.pe, crzuniga@utp.edu.pe, c19349@utp.edu.pe,
c22213@utp.edu.pe, u17211821@utp.edu.pe, u1510187@utp.edu.pe

Resumen— El advenimiento de la pandemia del COVID-19 ha demostrado claramente que las universidades peruanas están en riesgo de fraude y manipulación indebida de datos e información, ya que uno de los factores más vulnerables en los sistemas de información es el factor humano, lo que desencadena diversos ataques de ciberseguridad, por lo tanto, con el fin de mantener la continuidad de los procesos del negocio, en particular el proceso CORE de admisión, se ha detectado vulnerabilidades que amenazan la integridad, confianza y confidencialidad de la información de los postulantes en entidades públicas de educación superior, debido a la falta de políticas de seguridad, análisis e identificación de riesgos, diseño y arquitectura de redes vulnerables, privacidad y autenticidad de la información. En ese sentido, el presente trabajo propone como una alternativa de solución, el diseño de un modelo de arquitectura de seguridad de datos aplicando la tecnología Blockchain en los procesos de admisión de una universidad pública peruana en donde se realiza la propuesta inicial de la demostración del modelo utilizando la plataforma "Hyperledger Sawtooth", donde a partir del proceso de admisión AS-IS, se propone el proceso de admisión TO-BE donde se encontrarán todos los procesos virtualizados. Asimismo, una muestra de 45 colaboradores de universidades públicas peruanas concluyó que Blockchain es una tecnología disruptiva, para resguardar la seguridad de datos e información de activos digitales, proporcionando registros distribuidos y descentralizados.

Palabras clave— proceso de admisión, seguridad de datos, confidencialidad, Blockchain.

Summary— The advent of the COVID-19 pandemic has clearly demonstrated that Peruvian universities are at risk of fraud and improper manipulation of data and information, since one of the most vulnerable factors in information systems is the human factor, which triggers various cybersecurity attacks, therefore, in order to maintain the continuity of business processes, Therefore, in order to maintain the continuity of business processes, in particular the CORE admission process, vulnerabilities have been detected that threaten the integrity, trust and confidentiality of the information of applicants in public higher education institutions, due to the lack of security policies, risk analysis and identification, design and architecture of vulnerable networks, privacy and authenticity of information. In that sense, the present work proposes as an

alternative solution, the design of a data security architecture model applying Blockchain technology in the admission processes of a Peruvian public university where the initial proposal of the demonstration of the model is made using the "Hyperledger Sawtooth" platform, where from the AS-IS admission process, the TO-BE admission process is proposed where all the virtualized processes will be found. Likewise, a sample of 45 collaborators from Peruvian public universities concluded that Blockchain is a disruptive technology to safeguard the security of data and information of digital assets, providing distributed and decentralized records.

Keywords— admission process, data security, confidentiality, Blockchain.

I. INTRODUCCIÓN

Actualmente el sector educativo superior atraviesa un entorno de rivalidad constante y mejora continua, frente a este contexto y a todo el proceso de crecimiento en dicho sector surge la obstaculización debido a la pandemia y crisis sanitaria, el cual conllevó a frenar drásticamente la continuidad de lo antes mencionado. Es así cómo las universidades a nivel mundial se vieron en la posición de impulsar y llevar a cabo la continuidad de sus procesos de manera habitual [1].

Por la misma razón, se considera que existe la adecuación y obligación permanente de que todas las organizaciones adopten y se acoplen a los cambios que demanda la situación actual global [1][2], donde los procesos virtualizados de admisión requieren que su desarrollo sea soportado por una plataforma segura. Por otro lado, la UNESCO sostiene que, ante esta situación de vulnerabilidad sanitaria por la que atravesó el mundo, el sector educativo tuvo que garantizar la continuidad del derecho a la educación recurriendo a las TIC's [3], sin embargo, ante este abrupto cambio y el no haber previsto un escenario de tal magnitud, el 80% de países de alto ingreso pudo cubrir esta necesidad, situación que no ocurrió con los

países de bajos ingresos que se encontraron con un déficit de al menos el 50%, dejando así a la mitad de su población sin el derecho a la educación y a su continuidad.

Es así que, tomando lo expuesto anteriormente como punto de partida, surge la importancia de acoger una tecnología de vanguardia y alto nivel de seguridad. Por lo que se considera, a la tecnología Blockchain, como una solución ideal de los principales desafíos tales como el de lograr la inmutabilidad de datos, garantizando la transparencia, privacidad y confidencialidad de la información generando transacciones confirmadas que permiten llevar a cabo la responsabilidad y el no repudio de la información [4][5].

De la misma manera, frente a esta perspectiva en [6], aseguran la existencia de un gran valor que ofrece la tecnología Blockchain en cada proceso de cualquier organización en la cual se apliquen, de tal forma que, en escenarios de vulnerabilidad, conlleva a que las organizaciones asuman cambios en el ámbito tecnológico, esta tecnología la cual está proyectada como una herramienta digital descentralizada, con características de capacidad de almacenamiento y confidencialidad de datos e información [7]. Estas características van de la mano con mecanismos de consenso [8]. De esta forma, se permite integrar datos, asegurando la confianza y confidencialidad del proceso, por lo que, las personas inmersas al proceso y a la organización deben encontrarse preparadas para la adopción de dicha tecnología [1].

Frente a lo mencionado, se identifican las vulnerabilidades con las que cuentan las universidades del Perú en sus procesos de admisión, tales como el encontrarse expuestos a escenarios de fraude y manipulación de los datos de manera negligente. En tal sentido, en la presente investigación, se propone una alternativa de arquitectura de seguridad de datos utilizando tecnología Blockchain con el propósito de evaluar la confianza y confidencialidad de los datos que se obtienen en el proceso de admisión, asegurando que los datos empleados en este proceso no puedan ser modificados, ni manipulados de forma inducida, sin la previa aprobación de un consenso preestablecido de nodos que lo gestionan.

El presente trabajo está organizado de la siguiente manera: en la sección II se presenta el estado del arte de la implementación de Blockchain, en la sección III se describe la metodología para el levantamiento de la información, en la sección IV se exponen los resultados obtenidos y finalmente en la sección V las conclusiones.

II. ESTADO DEL ARTE

El periodo complicado que atravesó el contexto global a causa de la pandemia del COVID-19 originó que el ámbito educativo, optara sistemas de información, los cuales se desarrollaban en la virtualidad, con la intención de darle persistencia a sus procesos de negocio, sin embargo, no todos los requerimientos en cuanto a seguridad se vieron cubiertos [1].

Las brechas de inseguridad identificadas, por un lado van en relación con el empleo de sistemas centralizados, en los

cuales independientemente de que un individuo pertenezca o no al sistema, este tiene la facilidad de atacar un único punto de fallo, resultando ser muy vulnerable. En ese sentido, un claro ejemplo es el sector financiero, en la cual, a través de sus sistemas centralizados intervienen como un medio fiable garantizando transacciones seguras, más no la originalidad o fiabilidad de procedencia de las mismas [9], así también, existen complejos problemas en los sistemas portuarios en relación a la privacidad y confidencialidad de la información [10], esto debido a que los procesos de negocio son soportados por sistemas centralizados, quedando expuesto siempre una sola entrada vulnerable a los sistemas. Cabe añadir que ya existen algunas investigaciones para abordar de alguna manera la seguridad en los procesos de admisión de una entidad educativa, soportadas por sistemas con arquitecturas centralizadas. En [14] los autores afirman que los sistemas centralizados que poseen muchas capas eluden más la preocupación por la seguridad de los datos siendo un requisito primordial en el diseño de los sistemas enfocado a resguardar la información, Por otro lado en [15] los autores proponen un modelo el cual aporta valor a los procesos de negocio de una entidad educativa de tal forma que permita detectar a tiempo un ataque de denegación de ancho de banda de una red, dicho modelo basado en nodos auditores de latencia de tiempo de ejecución, sin embargo este no resguardaría la integridad de los datos e información si en caso un solo o una cantidad pequeña de documentos críticos de muchos postulantes se ven alterados.

Por ello, se afirma que los procesos de admisión de una universidad exigen de una plataforma que brinde las garantías necesarias de seguridad, confidencialidad y confianza [2]. Una muestra precisa, en donde se empleó a la tecnología Blockchain, reside en la investigación realizada en [6], donde se explica que Walmart e IBM mitigaron problemas de falta de transparencia y confianza para el proceso de seguimiento de producción de carne a través de un sistema Blockchain, el cual permitía hacer tracking en todas las fases del proceso.

Cabe reconocer que, el más grande aporte dado por Satoshi Nakamoto no exactamente fue el de Bitcoin, sino la columna vertebral que esta posee, la cual es Blockchain [8]. Blockchain es una de las tecnologías más vanguardistas que en la última década ha tenido mayor grado disruptivo, transformando y otorgando la seguridad meritosa a distintos segmentos del mercado global. Bajo esta premisa, resulta preciso afirmar que Blockchain posee una evolución significativa la cual se divide en tres fases: en primer lugar está todo lo relacionado al despliegue de las criptomonedas, seguidamente vienen las aplicaciones económicas en sectores de banca y finanzas que escala un poco más de ser transacciones comunes, finalmente la aplicación de Blockchain en sectores ajenos a la banca tales como educativos, ciencias, gubernamentales, industriales, entre otros [11]. En ese sentido, la tecnología Blockchain puede ser aplicada en distintos procesos en diferentes sectores. Este es el caso del sector salud, donde se pudo realizar un sistema de historia clínica basado en dicha tecnología, soportado en la plataforma Ethereum [12].

Previo a determinar la propuesta de solución del presente artículo se realizaron investigaciones acerca de algunos

modelos en donde plantean el uso de la tecnología Blockchain. En [2] detallan los investigadores a un nivel macro el modelo que utiliza tecnología Blockchain para resguardar la seguridad en los procesos de admisión en Instituciones Educativas, realizando la aplicación de contratos inteligentes los cuales bajo ciertas condiciones se ejecutarán permitiendo agregar bloques a la cadena, proponiendo así un Blockchain de tipo híbrida, sin embargo no detallan los niveles de los nodos que componen la red de cadena de bloques, a comparación de las investigaciones realizadas en [7] y [13] en donde plantean el empleo de la tecnología Blockchain para la digitalización de la contabilidad en competencias profesionales de la ciudadanía y la gestión descentralizada de cadenas de valor agrícolas usando tecnología Blockchain respectivamente, en las cuales se definen los nodos y permisos respectivos que componen la Blockchain [5].

En los casos expuestos anteriormente, se emplea el uso de plataformas de Blockchain como Bitcoin y Ethereum, siendo estas de tipo pública. Sin embargo, existen casos en donde dependiendo del reconocimiento previo de los requerimientos del proceso, se debe analizar el tipo de Blockchain que se necesita. Por ello se analizó y evaluó las fuentes de referencia, concluyendo así que, el modelo debe estar basada en una Blockchain de tipo híbrida usando la plataforma Hyperledger Sawtooth, la cual funge como una solución ideal para la implementación y desarrollo de libros contables distribuidos [16]. De una manera más específica se tiene por el lado público, los postulantes podrán escribir datos pertenecientes a ellos mismos y consultar su certificado HASH en la BLOCKCHAIN para verificar su información, mientras que por el lado privado, las entidades previamente establecidas como la SUNEDU (Superintendencia Nacional de Educación Superior Universitaria) y el RENIEC (Registro Nacional de Identificación y Estado Civil), harán el rol función de nodos validadores del proceso para añadir bloques a la cadena.

III. METODOLOGÍA

En cuanto a la metodología científica adoptada para el desarrollo del presente artículo, se tomó como punto de partida analizar y comprender el proceso de negocio, resultando necesario conocer el PROCESO DE ADMISIÓN AS-IS, para posteriormente proponer el PROCESO DE ADMISIÓN TO-BE.

Proceso de admisión AS-IS: Se identificaron las fases, actividades, tareas y actores correspondientes al proceso de admisión actual de una Universidad.

Proceso de admisión TO-BE: Tomando como base el proceso de admisión AS-IS, se evaluaron puntos y documentos críticos de mejora, alineándolo al avance tecnológico, permitiendo hacer más eficientes y eficaces el proceso.

Por otro lado, para la metodología tecnológica en relación con la prueba del modelo se usa la plataforma Hyperledger Sawtooth la cual permite desarrollar contratos inteligentes con reglas determinadas del proceso de negocio en distintos lenguajes de programación tales como, Java, Go, Python, Rust

entre otros [16]. Es así como, en la presente propuesta se toma la decisión de utilizar el lenguaje de programación Python en la versión 3.11.3 para la generación el Smart Contract que corresponde a la arquitectura de seguridad de datos que utiliza tecnología BLOCKCHAIN.

Proceso admisión AS-IS:

- a) Recepción del postulante : Atención presencial
- b) Ejecución del pago para el derecho de admisión: Pago físico.
- c) Inscripción del postulante: Documentos físicos.
- d) Rendimiento del examen de admisión: Examen físico.
- e) Evaluación y veredicto de resultados: Calificación física.
- f) Entrega de constancias de ingresos: Entrega Física.

Proceso admisión TO-BE:

- a) Recepción del postulante: Autogestión del postulante.
- b) Ejecución del pago para el derecho de admisión: Pago virtual.
- c) Inscripción del postulante: Documentos digitales.
- d) Rendimiento del examen de admisión: Examen Virtual
- e) Evaluación y veredicto de resultados: Calificación automatizada.
- f) Entrega de constancias de ingresos: Entrega virtual.

C. Propuesta del Modelo de Arquitectura de Seguridad de Datos usando Blockchain

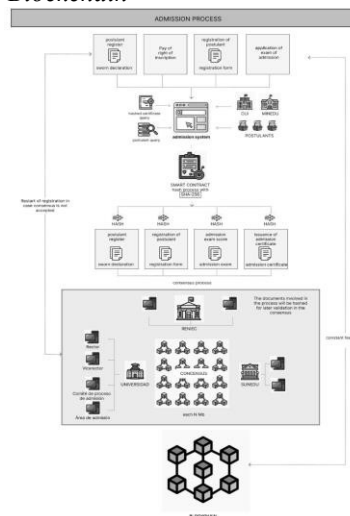


Fig. 1 Modelo de arquitectura de seguridad de datos con tecnología BLOCKCHAIN

La explicación del funcionamiento del modelo de arquitectura de seguridad de datos que utiliza Blockchain para garantizar la confianza y confidencialidad del proceso de admisión, es la siguiente:

- 1) *Recolección de los documentos críticos por cada fase importante del proceso de admisión.*
- 2) *HASHEO de los documentos críticos obtenidos de cada fase del proceso de admisión.*

- 3) Validación de información verídica respecto a los documentos críticos obtenidos.
- 4) Adición del bloque generado a la cadena de bloques Híbrida de la universidad.
- 5) Generación de credenciales BLOCKCHAIN para los documentos críticos correspondientes a cada postulante.

A partir de un análisis crítico y detallado de comparación entre las plataformas con mayor alcance para soportar procesos de tal magnitud, se concluyó que será Hyperledger Sawtooth la plataforma seleccionada para esta propuesta inicial debido a la flexibilidad que expone [16].

IV. RESULTADOS

En cuanto a los resultados obtenidos en la presente investigación, se precisa por un lado la realización de una simulación del modelo. Por otro lado, para complementar el estudio, se optó por aplicar una encuesta a los colaboradores que trabajan en el proceso de admisión, desde el punto de vista de tres perfiles distintos.

A. Demostración del modelo

En referencia a la simulación del modelo, para ver el funcionamiento de una Blockchain híbrida en una universidad bajo el proceso de admisión, tomando sus documentos críticos, se empleó la plataforma “Blockchain Demo: Hashes and Blocks”.

La Blockchain inicia con el primer bloque denominado el bloque “Genesis”, al cual no le precede ningún otro bloque, como puede ser apreciado en la figura 2.

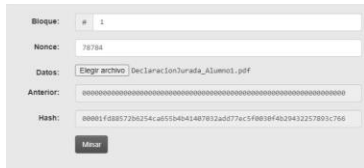


Fig. 2 Bloque número 1 de la Blockchain nativa híbrida

A.1 Bloque de código que realiza el HASHEO

A continuación, se presenta un extracto de código utilizado para realizar el HASHEO correspondiente de los archivos digitales críticos del proceso de admisión. Para el desarrollo de este algoritmo se utilizó el lenguaje de programación Python 3.11.3, junto a las librerías que ofrece la plataforma Hyperledger Sawtooth para el funcionamiento de la cadena de bloques.

```

1 import tkinter as tk
2 from tkinter import filedialog
3 import hashlib
4
5 def hash_file(file_path):
6     """Calculates the 512-bit SHA-256 hash of a file."""
7     hasher = hashlib.sha256()
8     with open(file_path, 'rb') as f:
9         while True:
10             chunk = f.read(1024)
11             if not chunk:
12                 break
13             hasher.update(chunk)
14     return hasher.hexdigest()
15
16 def choose_file():
17     """Opens a file dialog to choose a file."""
18     file_path = filedialog.askopenfilename()
19     file_hash = hash_file(file_path)
20     print(f'File path: {file_path}')
21     print(f'File hash: {file_hash}')
22
23 root = tk.Tk()
24 root.title('Blockchain App')
25
26 choose_file_button = tk.Button(root, text='Elegir archivo', command=choose_file)
27 choose_file_button.pack()
28
29 root.mainloop()

```

Fig.3 Algoritmo Python para el HASH

B. Perspectiva de colaboradores de un proceso de admisión

Se realizó una encuesta a colaboradores de una universidad peruana, que forman parte del proceso de admisión, el cual se basó en indicadores tales como; identificación y análisis de riesgos, diseño y arquitectura de red, políticas de seguridad, veracidad y privacidad de datos, además se tomó tres perfiles de colaboradores diferentes: Estratégico, Técnico y Operativo.

TABLA I
PRUEBAS DE NORMALIDAD PARA LA ENCUESTA

	Kolmogorov-Smirnov			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Profile	,308	45	,008	,756	45	,006
Likert_01	,302	45	,010	,781	45	,008
Likert_02	,302	45	,010	,781	45	,008
Likert_03	,254	45	,067	,833	45	,036
Likert_04	,370	45	,000	,752	45	,006

Los resultados pasaron por la prueba de Shapiro Wilk, debido a que se cuenta con una muestra de 45 encuestados. Luego, se aplicaron test paramétricos descriptivos. De acuerdo con lo observado en la tabla II, todos los parámetros seleccionados poseen un valor de p (significancia) mayor a 0.005, aceptando la hipótesis nula por lo que los datos siguen una distribución normal.

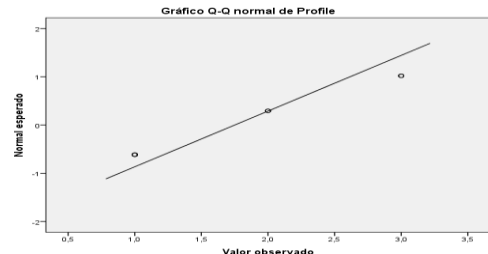


Fig. 4 Gráfico Q-Q normal de Profile

Tal como muestra la figura 6, con el gráfico Q-Q, se observa que los valores que toma el parámetro “Perfil del puesto” siguen una distribución normal.



Fig. 5 Indicadores del Perfil Estratégico

De acuerdo con la figura 6, los colaboradores pertenecientes al área Estratégica indican de acuerdo con la escala de Likert que el indicador de identificación y análisis de riesgos posee un nivel de 5, afirmando que ellos perciben que la implementación de Blockchain ayudaría mucho a poder identificar y analizar los riesgos.

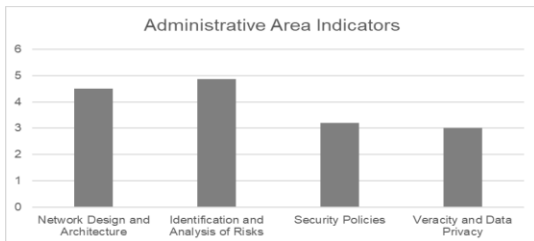


Fig. 6 Indicadores del Perfil Técnica

Según la figura 6, los pilares de Diseño y arquitectura de red además del análisis identificación de riesgos para el perfil operativo, también poseen una ponderación alta permitiendo reforzar y aseverar la decisión de implementar la tecnología Blockchain en el proceso de admisión. .

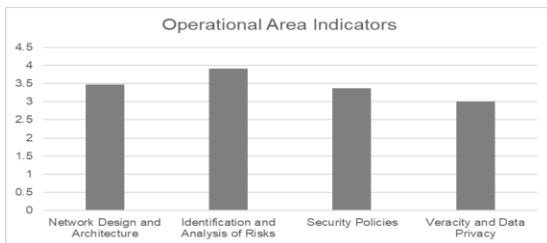


Fig. 7 Indicadores del Perfil Operativo

Finalmente, en la figura 7, para los colaboradores de perfil operativo también se coincide con que los pilares de diseño y arquitectura de la red además de identificación y análisis de riesgos poseen un ponderado alto siendo de 3.5 – 4.

V. CONCLUSIONES

En relación con el objetivo de la investigación se logró proponer y realizar el modelo de la arquitectura de seguridad de datos, soportada por la tecnología Blockchain cubriendo puntos con relación a la integridad y seguridad de la información del proceso de admisión. Se considera que el modelo realizado genera valor a las universidades conllevando a que se encuentren en mejora continua de la mano de las tecnologías de la información. De la misma forma, es preciso indicar que Blockchain es la tecnología ideal, de carácter disruptivo, para resguardar la seguridad de datos e información

de activos digitales, brindando un registro distribuido y descentralizado.

AGRADECIMIENTOS

Los autores del presente trabajo agradecen a la Universidad Tecnológica del Perú por el financiamiento recibido en todo el proceso de la investigación.

REFERENCIAS

- [1] S. S. Shah, A. A. Shah, F. Memon, A. A. Kemal, and A. Soomro, "Online learning during the COVID-19 pandemic: Applying the self-determination theory in the 'new normal,'" *Rev. Psicodidact.*, vol. 26, no. 2, pp. 169–178, 2021, doi: 10.1016/j.psicod.2020.12.004.
- [2] R. J. Kutty and N. Javed, "Secure Blockchain for Admission Processing in Educational Institutions," 2021 Int. Conf. Comput. Commun. Informatics, ICCCI 2021, pp. 27–30, 2021, doi: 10.1109/ICCCI50826.2021.9402654.
- [3] UNESCO, "Policy Brief: Education during COVID-19 and beyond," *Rev. Iberoam. Tecnol. en Educ. y Educ. en Tecnol.*, no. 26, p. e12, 2020, doi: 10.24215/18509959.26.e12.
- [4] N. Kumar, S. Tanwar, A. Nair, and R. Gupta, "Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges," *Inst. Eng. Technol.*, 2020, doi.org/10.1049/cmu2.12113
- [5] H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic, and M. Omar, "Trustworthy IoT Data Streaming Using Blockchain and IPFS," *IEEE Access*, vol. 10, pp. 17707–17721, 2022, doi: 10.1109/ACCESS.2022.3149312.
- [6] M. A. N. Agi and A. K. Jha, "Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption," *Int. J. Prod. Econ.*, vol. 247, no. June 2021, p. 108458, 2022, doi.org/10.1016/j.ijpe.2022.108458
- [7] S. Novikov, O. Mikheenko, H. Kulogina, and O. Kazakov, "Digitalización de la contabilidad de las competencias profesionales de la ciudadanía basada en tecnologías de libros de contabilidad distribuidos y contratos inteligentes." 2018, doi: 10.17323 / 1998- 0663.2018.4.43.53.
- [8] R. Zhang, R. Xue, and L. Liu, "Security and privacy on Blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, 2019, doi: 10.1145/3316481.
- [9] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging Trends in Blockchain Technology and Applications: A Review and Outlook," *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxx, 2022, doi: 10.1016/j.jksuci.2022.03.007.
- [10] Y. Liu, Z. Zhou, Y. Yang, and Y. Ma, "Verifying the Smart Contracts of the Port Supply Chain System Based on Probabilistic Model Checking," *Systems*, vol. 10, no. 1, 2022, doi: 10.3390/systems10010019.
- [11] M. Swan, "Blockchain blueprints for a new economy," vol. 293, no. 11, 2015.
- [12] R. A. Pava Díaz, J. N. Pérez Castillo, and N. V. L. Fernando, "Perspectiva para el uso del modelo P6 de atención en salud bajo un escenario soportado en IoT y Blockchain," *Tecnura*, vol. 25, no. 67, pp. 112–130, 2021, doi: 10.14483/22487638.16159.
- [13] J. Mosquera and N. Piedra, "Gestión Descentralizada de Cadenas de Valor Agrícolas Usando Tecnología Blockchain," *AGROBC*, 2020, doi: 10.21503/hamu.v7i3.2201.
- [14] L. L. Caimi, V. Fochi y F. G. Moraes, "Secure Admission of Applications in Many-cores", 2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS), Burdeos, Francia, 2018, pp. 761-764, doi: 10.1109/ICECS.2018.8618021
- [15] Rajesh, J. S., Ancajas, D. M., Chakraborty, K., & Roy, S. (2015). Runtime detection of a bandwidth denial attack from a rogue network-on-chip. Paper presented at the Proceedings - 2015 9th IEEE/ACM International Symposium on Networks-on-Chip, NOCS 2015, doi:10.1145/2786572.2786580
- [16] Hyperledger Sawtooth, «Hyperledger Sawtooth,» 2022. [En línea]. Available: <https://sawtooth.hyperledger.org/>.