



**UNIVERSIDAD POLITÉCNICA SALESIANA  
SEDE GUAYAQUIL  
CARRERA DE INGENIERÍA DE SISTEMAS**

**PROPUESTA DE ARQUITECTURA DE DATOS PARA LOS CERTIFICADOS DE  
VACUNACIÓN COVID-19 EN ECUADOR BASADO TECNOLOGÍA BLOCKCHAIN**

Trabajo de titulación previo a la obtención del  
Título de Ingeniero de Sistemas

AUTOR: EDER FABIÁN PEÑAFIEL SALAS

TUTOR: NELSON SALOMÓN MORA SALTOS

Guayaquil – Ecuador

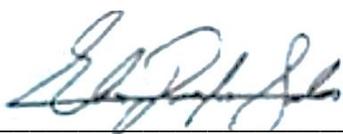
2022

**CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE  
TITULACIÓN**

Yo, **Eder Fabián Peñafiel Salas** con documento de identificación N° **0930172770** manifiesto que: Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 1 de junio del año 2022

Atentamente,



Eder Fabián Peñafiel Salas

0930172770

**CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE  
TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA**

Yo, **Eder Fabián Peñafiel Salas** con documento de identificación No. **0930172770**, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor(a) del Artículo Académico: “**Propuesta de arquitectura de datos para los certificados de vacunación COVID-19 en Ecuador basado tecnología blockchain**”, el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 1 de junio del año 2022

Atentamente,



---

Eder Fabián Peñafiel Salas

0930172770

## CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, **Nelson Salomón Mora Saltos** con documento de identificación N° 0909257800, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: **PROPUESTA DE ARQUITECTURA DE DATOS PARA LOS CERTIFICADOS DE VACUNACIÓN COVID-19 EN ECUADOR BASADO TECNOLOGÍA BLOCKCHAIN**, realizado por **Eder Fabián Peñafiel Salas** con documento de identificación N° **0930172770**, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 1 de junio del año 2022

Atentamente,



---

**Nelson Salomón Mora Saltos**

0909257800

## **DEDICATORIA**

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mi madre AMPARITO sé que nuestra distancia física no nos separó nunca, siento que estás conmigo y en una parte de alguna otra vida nos volveremos a topar, estoy seguro de que este momento hubiera sido tan especial para ti como lo es para mí. A mi ESPOSA E HIJO, a quien quiero y amo con mi vida, por compartir momentos significativos conmigo y por siempre estar dispuesta a escucharme y ayudarme en cualquier momento.

## **AGRADECIMIENTO**

Principalmente agradezco Dios, entre las metas más esperadas de mi vida, agradezco a mi familia, en especial a mi madre que siempre estuvo conmigo hasta en el último momento de su vida y fue quien confió en mí y aquí estoy con orgullo. También agradezco a mi familia esposa ANA VILLEGAS MUÑIZ MI PILAR fuerte y fundamental de mi vida y a mi alma de superación mi hijo EDER PEÑAFIEL VILLEGAS sin todos ellos no hubiera podido superar las dificultades en mi camino universitario, también a cada uno de los maestros que me impartieron sus conocimientos en cada aula.

## RESUMEN

La pandemia COVID-19 con millones de casos y decesos en todo el mundo obligó al distanciamiento social para disuadir la propagación del virus; la reapertura de los centros educativos, empresas y los traslados de las personas impuso el pedido de certificados de vacunación, tales certificados tienen vulnerabilidades. El objetivo es diseñar una arquitectura de datos para almacenamiento y seguridad de los certificados de vacunación COVID-19 en Ecuador basado tecnología blockchain. Se utiliza el enfoque de la investigación Empírico-Analítico, la investigación cualitativa, la técnica de la observación y la exploración de artículos científicos. El resultado es una arquitectura blockchain y un caso de estudio con costos básicos. Se concluye que la arquitectura propuesta en blockchain tiene bondades de seguridad y privacidad, facilita el traslado de las personas a nivel global, el modelo puede ser base para pasaportes y otros tipos de certificados con pequeñas actualizaciones.

**Palabras claves:** Blockchain, COVID-19, Certificado de Vacunación, Seguridad y Privacidad, Certificado Digital.

## ABSTRACT

The COVID-19 pandemic with millions of cases and deaths around the world forced social distancing to deter the spread of the virus; the reopening of educational centers, companies and the transfer of people imposed the request for vaccination certificates, such certificates have vulnerabilities. The objective is to design a data architecture for the storage and security of COVID-19 vaccination certificates in Ecuador based on blockchain technology. Empirical-Analytical research approach, qualitative research, observation technique and exploration of scientific articles are used. The result is a blockchain architecture and case study with basic costs. It is concluded that the proposed architecture in blockchain has security and privacy benefits, facilitates the transfer of people globally, the model can be the basis for passports and other types of certificates with small updates.

**Key words:** Blockchain, COVID-19, Vaccination Certificate, Security and Privacy, Digital Certificate.

## ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN.....	10
2. REVISIÓN DE LITERATURA .....	13
2.1. Tipos de certificados de vacunación.....	13
2.2. Concepto de blockchain.....	13
2.3. Ventajas de certificados digitales COVID-19 en blockchain .....	13
2.4. Certificados COVID-19 en blockchain.....	14
3. METODOLOGÍA.....	16
4. RESULTADOS .....	17
4.1. Analizar propuestas científicas para conocer certificados de salud en entorno blockchain mediante revisión bibliográfica. ....	17
4.2. Proponer una arquitectura de datos para los certificados de vacunación COVID-19 en Ecuador basado en tecnología blockchain. ....	20
4.3. Elaborar un caso de estudio en una ciudad para determinar los elementos y posibles costos mediante la descripción cualitativa y cuantitativa. ....	24
5. DISCUSIÓN .....	26
6. CONCLUSIÓN .....	27
REFERENCIAS .....	28

## 1. INTRODUCCIÓN

La pandemia de COVID-19 del año 2020 causó trastornos económicos y sociales a nivel mundial, por ser una enfermedad respiratoria el 11/marzo/2020 la Organización Mundial de la Salud (OMS) la declaró pandemia con las recomendaciones sobre distanciamiento, aislamiento y aseo personal para bajar la asistencia a los hospitales; la vacunación implementada en varios países contra esta pandemia tiene procesos como producción, distribución, gestión y vacunación; el certificado de vacunación (CV) entregado por inoculación impone restricciones de acceso a las actividades/reuniones sociales, existe el riesgo de la falsificación de estos certificados, aquí la confianza en un certificado es muy discutible (Khan et al., 2022).

Uno de los principales desafíos introducidos por la pandemia del COVID-19 es la línea base para información validada sobre la salud pública, esta información es necesaria para reforzar la movilidad nacional e internacional de las personas basado en un modelo seguro y privado; los gobiernos y organizaciones de muchos países mantienen campañas de vacunación para alcanzar la inmunización de su población. Además, existen algunas exigencias como solicitar el certificado de vacunación físico para la circulación de personas en los cines, estadios, restaurantes u otros lugares concurrencia (Karopoulos et al., 2021).

Las Tecnología de la Información (TI) son utilizadas en varias formas para detener la transmisión del virus, por ejemplo: la Organización Mundial de la Salud (OMS) recibió ayuda tecnológica, existen plataformas libres para el intercambio de información, sistematización en seguimiento de contactos, atención médica remota, utilización de robots, utilización de drones para provisiones médicas, chatbot, IoT para seguimiento de personas. También es utilizado en certificación de vacunas para evitar la propagación de COVID-19, porque los gobiernos aplican protocolos a las personas que presenten el certificado (Abubakar et al., 2021).

Blockchain es utilizado en áreas de seguimiento y autenticidad, por ejemplo en aplicaciones informáticas de cadena de suministro, trazabilidad y certificaciones; la descentralización de blockchain facilita la autenticación, reduce el tiempo y aumenta la rapidez de las transacciones; blockchain valida la autenticidad de bienes o la fuente de datos de documentos (certificados); existe buen interés para que el certificado se desarrolle en colaboración pública y privada, un certificado de vacunación validado genera buena aceptación en las personas (Abuhashim et al., 2021). Se consideran un gran desafío la sensibilidad y permanencia de las pruebas realizadas en los exámenes/pruebas/certificados médicos, la escalabilidad de la pandemia COVID-19 tiene

secuelas financieras a nivel global, por lo tanto es meritorio que la certificación de vacunación o experimento de anticuerpos sea sólida por su extensa demanda a nivel global; además existen implicaciones legales, sociales, políticas y éticas por esta certificación de vacunas (Eisenstadt et al., 2020). La tecnología blockchain es utilizada en sectores como gobierno, comercio, financiero, industria, la educación y la salud (Abid et al., 2021).

En Ecuador para la verificación de la vacunación de una persona se solicita el documento físico y otra alternativa es la revisión en la página web (MSP, 2022) del Ministerio de Salud Pública con el número de cédula y fecha de nacimiento de la persona.

Debido a esta reciente pandemia o una futura pandemia, la certificación tiene gran importancia y lugar porque los gobiernos responden por la salud de los ciudadanos y empresas privadas responden por la salud de sus empleados.

Este documento se centra en el certificado de vacunación digital basado en blockchain, porque un certificado de vacunación es un documento sensible, con alto valor que conserve la privacidad, que no sea falsificable, administración sencilla, verificación sencilla y escalable a millones de personas. El diseño que se propone tiene enfoque descentralizado con datos cifrados que permanecen en una cadena de bloques/transacciones que son inmutables.

Para permitir la libre movilidad de personas en varios países piden el certificado de vacunación COVID-19 para continuar sus actividades regulares y asistencia a eventos masivos (Khan et al., 2022), (Karopoulos et al., 2021).

Los certificados de vacunación físico son simples papeles que pueden ser impresos o falsificados, en la misma manera, los certificados digitales de vacunación deben ser extremadamente inmunes al fraude, sencilla verificación, sencilla emisión, mantener la privacidad y mantener la interoperabilidad, es necesario que las infraestructuras de datos tengan seguridad, privacidad y escalabilidad (Karopoulos et al., 2021).

Un documento electrónico maximiza la interoperabilidad y minimiza la inconsistencia de los datos de varios lugares como gobiernos u hospitales.

Los certificados de vacunación minimizan la propagación del virus para que los países abran sus economías, pero es necesaria la seguridad del certificado en mantener los datos en forma

privada y precisa para diferentes aplicaciones informáticas que consultan los datos; existe la venta abierta de certificados entre 20 y 200 dólares americanos, en Mayo-2021 Irlanda tuvo ataques a su sistema informático de salud, Australia tiene vulnerabilidades en su certificado digital, las aplicaciones informáticas son centralizadas y sin privacidad; con estos antecedentes es necesaria una infraestructura apropiada para los certificados de vacunación (Abubakar et al., 2021). Las aplicaciones centralizadas son vulnerables y dan paso a datos defectuosos, Blockchain se utiliza en certificación de vacunación y así maximizar la confianza durante el proceso de inoculación, el certificado no caduca en la red, los datos son inmutables y el certificado se comparte entre las participantes de la red descentralizada (Abuhashim et al., 2021).

El objetivo es diseñar una arquitectura de datos para almacenamiento y seguridad de los certificados de vacunación COVID-19 en Ecuador basado tecnología blockchain.

## 2. REVISIÓN DE LITERATURA

### 2.1. Tipos de certificados de vacunación

En el tiempo de la pandemia de COVID-19 para que las personas vuelvan a sus actividades fue pedirles el certificado que avale su inmunidad o vacunación; existen tres tipos de certificados en salud: a) certificado de vacunación que avala que la persona tiene la vacuna (CV); b) certificados de pruebas diagnósticas que avala el estado de salud de la persona (CP); y c) certificados de inmunidad que avalan que la persona fue infectada y tiene de anticuerpos (CI) (Karopoulos et al., 2021).

### 2.2. Concepto de blockchain

Es un libro de registros que resiste la manipulación aun en los momentos que el libro está en crecimiento, además los registros están distribuidos y copiados en nodos de la red, cada registro contiene una marca de tiempo; para mantener los registros seguros se utiliza algoritmos criptográficos, la firma cifrada y un consenso distribuido; otras funcionalidades de blockchain son transparencia, ocultar identidad, la tolerancia a fallas, la integridad de los datos y ejecución en un ambiente sin confianza. Además utiliza Contratos Inteligentes que verifica las reglas configuradas en la red blockchain, estas reglas ejecutan los términos predefinidos en un código de programa. Blockchain es un libro transacciones/registros que están distribuidos en una cadena organizada en bloques, estos se comparten y replican en forma sincronizada entre los nodos de la red (Abid et al., 2021).

Existen tres controles de permisos: a) Blockchain pública en que todos leen y mantienen el libro de registros, b) Blockchain consorcio tiene acuerdos para conservar el libro de registros, c) Blockchain privada que una sola organización controla toda la red.

### 2.3. Ventajas de certificados digitales COVID-19 en blockchain

Son documentos confiables para verificación de personas vacunadas o resultado negativo, agiliza muchas actividades en el tiempo de pandemia (Karopoulos et al., 2021), reducción de certificados falsos, reducción de datos falsos, aumento de confiabilidad en los certificados (Hasan et al., 2020), mantiene la integridad de datos, mantiene los datos en forma inmutable, permite a las personas control sobre sus propios datos, los datos personales están cifrados, asigna credenciales a los usuarios, verificación de los certificados, permite seleccionar a los destinatarios para compartir datos (Abid et al., 2021), no hay extracción de información por

parte de terceros, sencillez en la verificación por ser un recurso público, confirmaciones confiables en las fronteras, trazabilidad en los reclamos, seguimiento de los dispositivos que son modificados (Bansal et al., 2020).

#### 2.4. Certificados COVID-19 en blockchain

En Canadá (Lemmon, 2021) se implementó una aplicación para registrar a personas vacunadas o con resultados negativos, el CV solo es registrado por 448 centros de salud autorizados por el gobierno; además cumple estándares internacionales y protocolos de identificación, las credenciales son propiedad de las personas y no permite falsificación, actualización o suplantación de identidad.

El gobierno de Estonia (Hernández-Ramos et al., 2021), en el documento se enfoca en los CV basado en blockchain-Hyperledger y en los certificados generados por OMS, se utiliza un ambiente de identificación que enlaza la vacunación de una persona con su propia identidad para que el CV mantenga la privacidad, la verificabilidad, escalabilidad e identificación descentralizada; además el sistema permite compartir los datos de manera selectiva preservando la privacidad de las personas.

En la arquitectura de (Eisenstadt et al., 2020) se propone almacenar los CV y CI basados en blockchain-Ethereum, el certificado digital contiene datos de identificación física y del certificado de salud, la persona vacunada guarda sus datos en una estructura sólida, además la propuesta hace énfasis en mantener la privacidad.

El diseño e implementación de (Abid et al., 2021) para los documentos digitales que guardan CV, CP y CI basados en blockchain-Ethereum permite mantener los certificados con privacidad, escalabilidad, seguridad e integridad, además evita la falsificación, la entrada de terceros sin permisos y eliminación de los datos, también la población y derechos de las personas están protegidas en esta propuesta.

La propuesta de (Hasan et al., 2020) protege la identidad bajo el cifrado y el almacenamiento descentralizado, los documentos que se guardan son CV y CI basados en blockchain-Ethereum, la identidad médica de las personas se mantiene con respuestas veloces y alta confianza en las autoridades; esta propuesta minimiza los datos falsos, aumenta la confianza y ayuda a minimizar la propagación del virus.

En (Bansal et al., 2020) se propone utilizar la tecnología blockchain para almacenar CI, descartar la falsificación de datos y minimizar las personas que desean infectarse; para esto los pacientes se registran en la red gestionada por el gobierno, además los laboratorios y hospitales deben pertenecer a esta red porque ellos suben la información de los pacientes, en caso que el paciente tenga anticuerpos el sistema genera y entrega un token temporal al paciente; la red utiliza la confirmación biométrica para acceso de las personas, esto asegura la privacidad y el anonimato.

La propuesta de (Chaudhari et al., 2021) mantiene la privacidad, y la identificación del usuario es por medio del iris de la persona, el CV e identidad anónima se almacenan en blockchain, aunque el rendimiento y almacenamiento pueden estar comprometidos durante el crecimiento de usuarios a nivel de país o global.

Se propone un CP (Constantinos Marios Angelopoulos, 2020) para turistas internacionales y con ello reactivar el turismo para minimizar el riesgo de contagio, el framework se basa en blockchain-privado con una autoridad para la emisión de CP en una red distribuida en las aplicaciones informáticas de salud para extranjeros, además de la verificación de las autoridades fronteras y empresas aéreas.

La solución en blockchain de (Gruener, 2020) protege la privacidad y es fuerte ante los fraudes, las personas gestionan el control de sus datos basados en una arquitectura descentralizada para los CP y CI; utilizan estándares de identificación para los certificados y esta propuesta presenta como principal ventaja la identificación descentralizada y certificados verificables.

El documento (Hicks et al., 2020) digitaliza el CI en un protocolo descentralizado con el objetivo de mantener la privacidad y emisión de los certificados; las pruebas e implementación disminuyen los riesgos y aumentan la seguridad de los datos, esta propuesta utiliza protocolos para disminuir la discriminación de las personas.

### 3. METODOLOGÍA

Se utiliza el enfoque de la investigación Empírico-Analítico para alcanzar el objetivo y validez de la ciencia, además de comprobar los enfoques hipotéticos de las referencias con la descripción de los hechos. Se utiliza la investigación Cualitativa para analizar las características de otras propuestas en blockchain y describir las cualidades, propiedades o componentes de nuestra arquitectura en esta propuesta. Se utiliza la técnica de la Observación para entender otros modelos blockchain, obtención directa de datos desde las referencias científicas y obtención de datos sobre el certificado de vacunación en Ecuador. Se utiliza la Exploración de artículos científicos que proporcionan información sobre certificaciones COVID-19 realizadas en blockchain.

Para la proponer la arquitectura de datos, se utiliza el método Descriptivo para expresar la percepción de los artículos científicos relacionados a blockchain, COVID-19 y certificados; además para determinar y describir los elementos de la arquitectura como: participantes/involucrados, tipo de plataforma blockchain, nodos, estructura de datos del certificado, funciones de la red blockchain, vía de comunicación, aplicaciones informáticas y almacenamiento.

Se realiza un Caso de estudio para describir la implementación hipotética de la arquitectura en una ciudad de Ecuador, se identifican los participantes como Ministerio de Salud Pública, institutos de investigaciones, hospitales, centros de salud, coordinación de tecnologías de información, doctores y ciudadanos; se determinan las herramientas de software, se determina el hardware mínimo, se determina costos mínimos en dólares americanos que tendría la arquitectura en su posible implementación.

## 4. RESULTADOS

### 4.1. Analizar propuestas científicas para conocer certificados de salud en entorno blockchain mediante revisión bibliográfica.

De la revisión bibliográfica se obtuvieron 30 artículos sobre blockchain relacionados a certificados de salud.

De los 30 artículos, el 33% de los proyectos utilizaron blockchain privado, el 63% utilizaron blockchain público y 4% utilizó blockchain consorcio, es decir la mayoría de los proyectos se dirigen a tipo público, ver Figura 1.

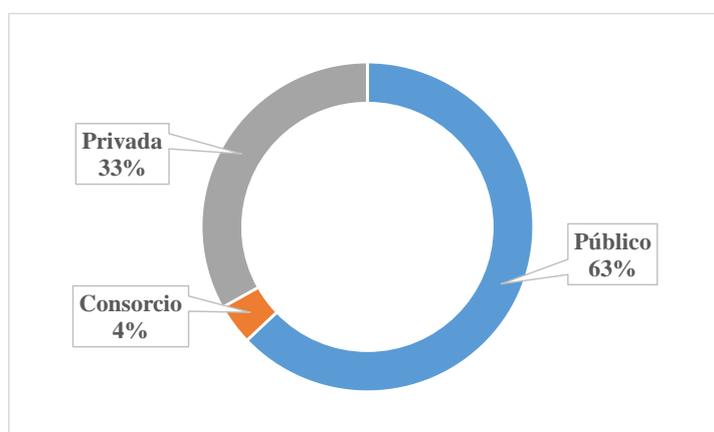


Figura 1. Tipos de blockchain utilizados

Los proyectos se dirigieron a diseñar o implementar uno o más tipos de certificados contra COVID-19, de los 30 artículos, el 65% realizaron modelos sobre certificado de vacunación, el 19% realizaron modelos sobre certificados de pruebas y el 16% realizaron pruebas sobre certificados de inmunidad; entre los 30 proyectos existen 5 que realizaron certificados sobre 2 de estos tipos, y solo un proyecto realizó certificados para los tres tipos, ver Figura 2.

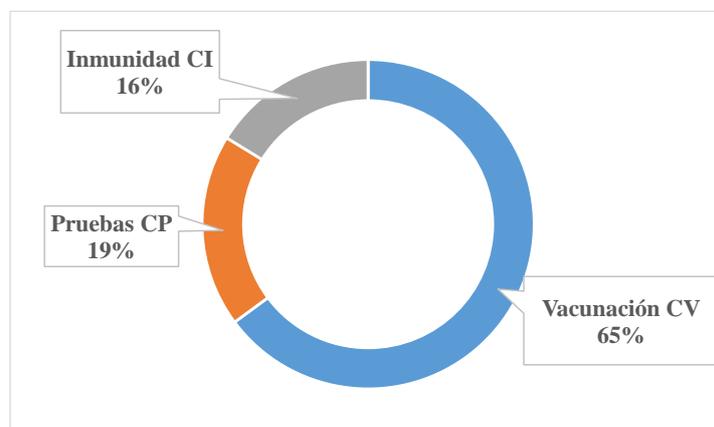


Figura 2. Tipos de certificado

El 40% de los proyectos presentaron una arquitectura en la propuesta del documento y el otro 60% no presentaron ningún modelo o arquitectura.

El 63% de los proyectos realizaron la codificación o implementación de sus propuestas y el otro 27% no implementaron nada.

El 50% de los proyectos realizaron su propuesta para algún gobierno o consideraron a los gobiernos, y el otro 50% no nombra al gobierno.

El 37% de los proyectos utilizan código QR en la asignación del certificado hacia el ciudadano, y el 63% no nombra el código QR.

El 77% de los proyectos hacen énfasis en la privacidad de las personas y el 23% no nombra la privacidad.

El 73% de los proyectos hacen énfasis en la seguridad de los datos y el 27% no nombra la seguridad.

La tabla 1 representa el resumen de proyectos blockchain en certificados de Covid-19.

Nota: el estudio (Mithani et al., 2022) contiene 8 trabajos realizados de blockchain sobre certificados.

Tabla 1. Proyectos en blockchain

N	PROY	ARQ	IMPLEMENTADO	GOBIERNO	QR	PRIVACIDAD	SEGURIDAD
1	(Lemmon, 2021)	NO	SI	SI	SI	NO	SI
2	(Hernández-Ramos et al., 2021)	NO	NO	SI	NO	SI	NO
3	(Eisenstadt et al., 2020)	SI	NO	NO	SI	SI	NO
4	(Abid et al., 2021)	SI	SI	SI	SI	SI	SI
5	(Hasan et al., 2020)	SI	SI	NO	NO	NO	NO
6	(Bansal et al., 2020)	NO	NO	SI	NO	SI	NO
7	(Chaudhari et al., 2021)	NO	NO	NO	NO	SI	SI
8	(Constantinos Marios Angelopoulos, 2020)	SI	NO	SI	NO	SI	SI
9	(Gruener, 2020)	NO	NO	SI	NO	SI	NO
10	(Hicks et al., 2020)	NO	SI	SI	SI	SI	SI
11	(Abdi & Herbert, 2018)	NO	NO	NO	NO	NO	SI
12	(Wang et al., 2020)	SI	SI	SI	NO	NO	SI
13	(Barati et al., 2021)	SI	SI	SI	NO	NO	SI
14	(Madhwal et al., 2021)	SI	SI	SI	NO	NO	SI
15	(Wu et al., 2019)	SI	SI	NO	NO	NO	SI
16	(Mithani et al., 2022)	NO	SI	NO	SI	SI	SI
17	(Mithani et al., 2022)	NO	SI	NO	SI	SI	SI
18	(Mithani et al., 2022)	NO	SI	NO	SI	SI	SI
19	(Mithani et al., 2022)	NO	SI	NO	SI	SI	NO
20	(Mithani et al., 2022)	NO	SI	SI	SI	SI	NO
21	(Mithani et al., 2022)	NO	SI	NO	NO	SI	NO
22	(Mithani et al., 2022)	NO	NO	NO	NO	SI	SI
23	(Mithani et al., 2022)	NO	SI	SI	NO	SI	SI
24	(Shamsi et al., 2020)	NO	NO	NO	SI	SI	SI
25	(Dima et al., 2021)	SI	SI	SI	NO	SI	SI
26	(Cao et al., 2022)	SI	NO	SI	NO	SI	SI
27	(INMUNITY, n.d.)	NO	SI	NO	SI	SI	SI
28	(Alabdulkarim et al., 2021)	SI	SI	NO	NO	SI	SI
29	(Deka et al., 2020)	NO	SI	NO	NO	SI	SI
30	(Ishengoma, 2021)	SI	NO	SI	NO	SI	SI

Fuente: Elaboración propia.

Entre los 30 artículos, 18 nombran las autoridades para control del certificado, 17 nombran los centros de salud aplicación de la vacuna y emisión del certificado, 5 nombran los laboratorios en la toma de muestras, 3 nombran a los verificadores como aeropuertos o lugares de reunión, 1 nombra a las farmacias para aplicación de la vacuna, y 1 nombra los doctores para seguimiento de la salud, ver Figura 3.

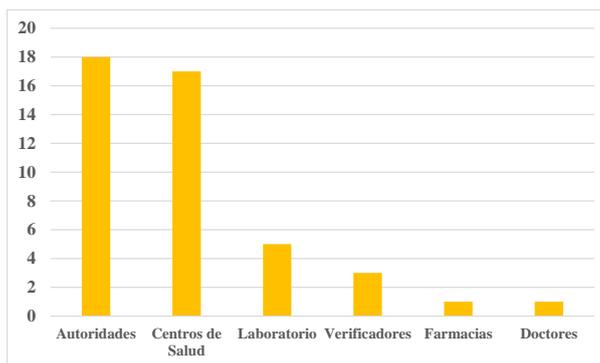


Figura 3. Interesados en los modelos blockchain

Entre los 30 artículos, 18 nombran el Smart Contract en sus propuestas, por consiguiente se entiende que 18 utilizan un almacén de datos, 17 nombran el certificado de autorización para acceso a los usuarios, 15 nombran utilizar algún programa de interface visual, y 9 nombran los nodos que participan en los modelos como hospitales, centros de salud, autoridades, ver Figura 4.

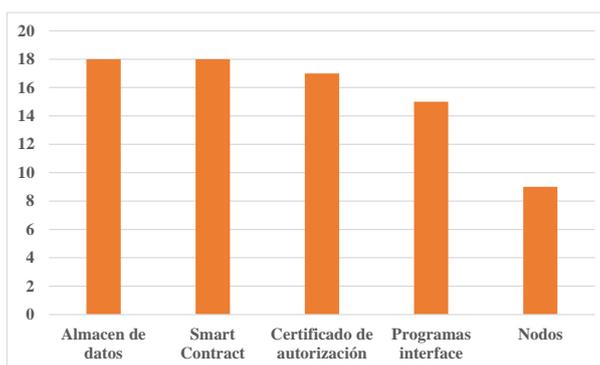


Figura 4. Componentes en los modelos blockchain

#### 4.2. Proponer una arquitectura de datos para los certificados de vacunación COVID-19 en Ecuador basado en tecnología blockchain.

Se propone una arquitectura basada en blockchain para almacenar de manera segura e inmutable los certificados de vacunación, con los siguientes elementos:

La red blockchain está formada por dos plataformas. La primera plataforma es Hyperledger que contiene como integrantes al Ministerio de salud, hospitales y centros de salud, además cada actor contiene una copia del Smart Contract, Ledger y Certificado de Autenticación, otro elemento es el Access Control y Proveedor de Servicios. La segunda red es Ethereum que contiene los ciudadanos, Auditores y Otros interesados, esta red es pública no necesita ninguna

credencial, esta red es solo para consulta a los certificados y pueden acceder gran cantidad de personas o instituciones, ver Figura 5.

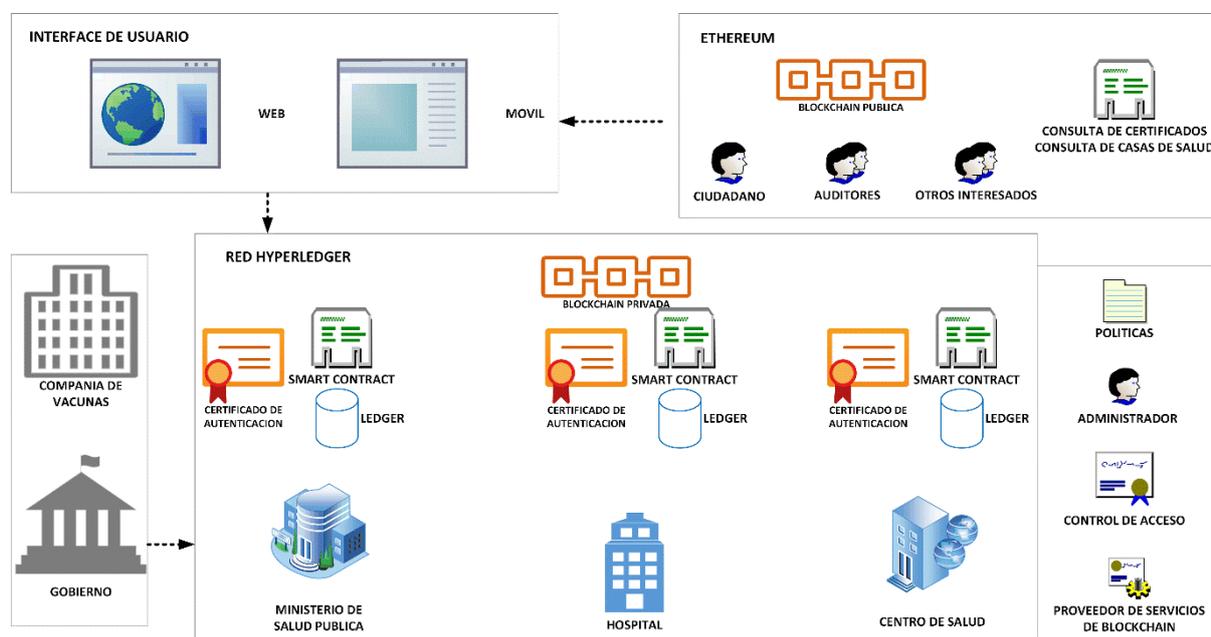


Figura 5. Arquitectura en blockchain

## Actores

**Compañía de vacuna:** Es la empresa que genera y entrega las vacunas al gobierno, su acceso es solo consulta de cantidad de vacunados, se recuerda que las vacunas son solo entregadas a los gobiernos.

**Gobierno:** En esta arquitectura sólo se encarga de la distribución de las vacunas, entrega de la logística y registro independiente de la distribución.

**Ministerio de Salud:** El ministerio crea los accesos, los permisos y el contrato inteligente en la red, habilitar el acceso a los hospitales y centros de salud que aplican las vacunas, el ministerio firma una transacción para autorizar o des autorizar a hospitales/centros de salud. Además, contiene una copia de la base de datos del Registro Civil para verificación de los datos de cada ciudadano.

**Hospital y centros de salud:** Luego que el ministerio registra y autoriza un hospital o centro de salud, este genera el certificado en blockchain y entrega el certificado de vacunación al ciudadano; es decir para cada certificado digital se realiza la inoculación.

Otros interesados: Son las entidades verificadoras, es decir cualquier entidad como aeropuerto, aduana, clínica, escuelas, universidades, restaurantes, centro comercial, cines, etc, que está en libertad de comprobar el certificado de vacunación mediante una interfaz de usuario que accede al blockchain.

Ciudadano: Es la persona que recibe la vacuna por parte del hospital o centro de salud, luego de la inoculación se crea en la cadena de datos el certificado.

**Smart Contract:** En esta propuesta el Ministerio de Salud es el propietario del Smart Contract que guarda los datos, autoriza a los hospitales/centros de salud, obtiene los datos del registro civil, consulta el certificado.

Las siguientes funciones descritas pertenecen al Smart Contract:

F1) Registro Hospital o Centro Salud: Solo el ministerio de salud puede ejecutar esta función y enviar los parámetros nombre, dirección, punto de vacunación, puntos de vacunación. Los datos entregados se almacenan en el ledger del blockchain, el ledger almacena los datos en forma de clave-valor.

F2) Consulta Hospital o Centro Salud: Entrega los datos relacionados al hospital o centro de salud que está en proceso de vacunación.

F3) Certificado de Vacunación: El hospital o centro de salud que está autorizado a vacunar debe registrar la inoculación de la persona, esta función registra: país de vacunación, el número de cédula, código de huella dactilar, fecha de vacunación, lugar de vacunación, tipo de vacuna, número de dosis, persona que suministra la vacuna, lote; considerar que la fecha de la vacunación se toma del servidor.

F4) Generar código QR: Esta función genera y entrega un código QR a la persona vacunada, para esto se recibe como parámetro: el número de cedula y código de huella dactilar; la función envía el código QR al usuario.

F5) Consulta de Certificado: Esta función es solo consulta pública para cualquier institución o persona, la consulta es por un código QR que la persona vacunada le entrega al verificador, se puede enviar a la consulta todos los certificados de vacunación del ciudadano, para esto se requiere como parámetro el número de cedula.

La lectura de datos en esta arquitectura no requiere de pagos ni tarifas, la lectura es sencilla y rápida por la capacidad de obtención de datos del Smart Contract que es instantáneo y sin costo monetario, el Smart Contract solo necesita el número de certificado o número de cédula de identidad. El blockchain de manera interna registra los accesos y registra las operaciones realizadas por cualquier actor; el Smart Contract es implementado por el administrador del Ministerio de Salud; el Smart Contract genera los datos de auditoría que los actores procesan en el sistema.

**Interfaces:** La interfaz de usuario es un front-end para los vacunadores, ciudadanos y otros interesados puedan interactuar con la plataforma blockchain; estas interfaces se conectan con el Smart Contract. La interfaz de ciudadanos puede consultar los certificados y generar los códigos QR; la interfaz de vacunadores puede ingresar los datos de cualquier persona vacunada y puede consultar; la interfaz de otros interesados puede consultar los certificados de vacunas de un ciudadano, previa recepción del código QR que pertenece al ciudadano.

**Roles:** Se definen tres roles para esta arquitectura: a) Administrador que inicia la red, registra a los demás usuarios y subadministradores, entrega los certificados de autenticación al Ministerio de Salud, hospitales y centros de salud. b) Auditor que solo puede consultar las transacciones y mantener la supervisión y optimización de la seguridad del sistema. c) Ciudadanos que consultan sus propios certificados y generan el código QR para que otros puedan consultar su certificado. d) Otros que sólo pueden consultar el certificado de vacunación con el permiso del código QR del ciudadano.

El ledger es el repositorio de datos, está en CouchDB que es el repositorio descentralizado para almacenamiento y es una biblioteca de estado de usuario, esta base de datos descentralizada realiza la gestión de la información que pertenece a los usuarios en forma rápida y segura

**Certificado de Autenticación:** Hyperledger permite al administrador generar Certificados de Autenticación que son credenciales para entrar a la red blockchain, esta credencial es un usuario y contraseña que están almacenadas y encriptadas en la red; en este caso el administrador genera credenciales para el ministerio de salud, hospitales y centros de salud.

4.3. Elaborar un caso de estudio en una ciudad para determinar los elementos y posibles costos mediante la descripción cualitativa y cuantitativa.

Software: El software que se necesita es de libre licencia o gratuito, para esto se necesita lo siguiente:

Sistema Operativo Ubuntu Server para instalación en el servidor que contiene la configuración inicial de la red (Ubuntu-Server, 2022).

Sistema operativo Ubuntu Desktop para instalación en las computadoras de los clientes en el ministerio de salud, hospital y centros de salud (Ubuntu-Desktop, 2022).

Hyperledger es la parte privada de la red blockchain, se recomienda la versión Hyperledger Composer que contiene un framework para implementación de la privada, esta red debe estar en un servidor principal (Hyperledger-Fundation, 2022).

Ethereum es la parte pública de red blockchain, esta red debe estar en un servidor secundario (Ethereum-Oficial, 2022).

Java para el desarrollo de aplicaciones web y aplicaciones móviles (Java-Netbeans, 2022).

Para el desarrollo de la aplicación web y aplicación móvil se consideran dos recursos, ver Tabla 2.

Tabla 2. Perfiles recomendados

Recurso	Perfil	Meses	Sueldo	Subtotal
Experto en blockchain Ethereum e Hyperledger	Ingeniero en sistemas con experiencia en arquitecturas distribuidas y blockchain	3	1500	4500
Desarrollador en aplicaciones web y móvil	Egresado en sistemas con experiencia en Java Enterprise Edition, HTML, CSS y Xamarin	3	900	2700
			Total	7200

Fuente: Elaboración propia.

Hardware: para este caso de estudio solo se considera el ministerio y un hospital; se asume que el ministerio y hospital tiene red física interna (LAN) y conexión a internet; el hardware recomendado con precios promedio del mercado se presenta en la Tabla 3:

Tabla 3. Equipos recomendados

Hardware	Ubicación	Característica	Cant.	Precio	Subtotal
Servidor Hyperledger	Ministerio	CPU: HP proliant ML 30 Intel Xeon, Monitor Led 19 pulgadas	1	1228.64	1228.64
Servidor Ethereum	Ministerio	CPU: HP proliant ML 30 Intel Xeon, Monitor Led 19p	1	1228.64	1228.64
Computador Cliente	Hospital	CPU: Core i5, 8 Gigas RAM, Disco Sólido 250, Monitor Led 19 pulgadas	1	597.00	597.00
				Total	3054.28

Fuente: Elaboración propia.

El proyecto tendría un costo básico de 10254.28 dólares americanos durante 3 meses que dura el desarrollo e implementación. Está considerado solo un hospital, cada hospital o centro de salud debe tener su computador para ingreso de los inoculados, en caso que se aumenten más hospitales también deben aumentarse computadores de escritorio.

## 5. DISCUSIÓN

Este documento describe una plataforma basada en Blockchain para creación y conservación perpetua de certificaciones de vacunas COVID-19, el sistema utiliza ledger y Smart Contract para conservar de forma segura los datos de los ciudadanos y optimizar el acceso de todos los actores; esta arquitectura se beneficia de las características únicas de blockchain

No está al alcance de esta investigación la implementación del certificado de vacunación. El gobierno solo se encarga de la distribución de las vacunas, esta propuesta no se considera el registro en la distribución o inventario de las vacunas. Esta propuesta no sólo se limita al área de salud, esta arquitectura puede aplicarse a otros sectores como certificados de calidad, certificados de educación, certificados de empleo, entre otros.

Blockchain puede tener un impacto positivo en áreas no comerciales como educación, trabajo, salud médica precisa, minimizar la pobreza, minimizar la falsificación, aumentar la seguridad alimentaria, generar bienestar público, la colaboración social, entre otros.

El proyecto tendría un costo básico de 10254.28 dólares americanos durante 3 meses que dura el desarrollo e implementación. El costo de recursos humanos y software no varían si el proyecto es para un solo hospital o para decenas de hospitales.

Nuestra arquitectura en esta propuesta tiene las características principales de blockchain como seguridad, privacidad para el ciudadano, confidencialidad para el ciudadano, integridad de la información y disponibilidad en todo momento. La arquitectura es escalable porque blockchain es una red distribuida cada hospital o centro de salud mantiene una copia del ledger o base de datos distribuida, esto da paso a certificados digitales a gran escala.

El desafío pendiente es el rendimiento de la arquitectura durante la ejecución, el aumento de los nodos y despliegue de la plataforma; se sugiere una red 100 Mbps, los CPU deben ser más potentes y aumento de memoria, puede existir límites en la cantidad de transacciones por segundo.

La plataforma blockchain es interesante porque puede satisfacer las necesidades y vulnerabilidades en la cadena de suministro de vacunas, y dar seguridad a los datos en el almacenamiento, trazabilidad y administración de inventario.

## 6. CONCLUSIÓN

Se conoció que otras 30 propuestas científicas en certificados de salud sobre blockchain hacen énfasis en redes públicas, arquitecturas, implementaciones, relación con gobierno, privacidad y seguridad.

El certificado de vacunación puede ser una Credencial Digital Legal para cualquier ciudadano del mundo y este indica su inoculación ante COVID-19; esta arquitectura propuesta en este documento es factible en generar confianza y minimizar la falsificación, las características de blockchain hacen que el certificado sea seguro, privado, rastreable e inmutable.

Este documento entrega una descripción técnica general mediante el caso de estudio para conocer los costos mínimos, recursos humanos y equipos; esto contribuye de manera general el desarrollo del certificado de vacunación en blockchain.

## REFERENCIAS

- Abdi, S., & Herbert, J. (2018). An algorithm for distributed certificate chain discovery in open environments. *Proceedings of the ACM Symposium on Applied Computing, 13-17-April*, 2292–2298. <https://doi.org/10.1145/2695664.2695676>
- Abid, A., Cheikhrouhou, S., Kallel, S., & Jmaiel, M. (2021). NoVIDChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. *Software: Practice and Experience, January*, spe.2983. <https://doi.org/10.1002/spe.2983>
- Abubakar, M., McCarron, P., Jaroucheh, Z., Al Dubai, A., & Buchanan, B. (2021). Blockchain-based Platform for Secure Sharing and Validation of Vaccination Certificates. *2021 14th International Conference on Security of Information and Networks (SIN)*, 1–8. <https://doi.org/10.1109/SIN54109.2021.9699221>
- Abuhashim, A. A., Shafei, H. A., & Tan, C. C. (2021). Block-VC: A Blockchain-Based Global Vaccination Certification. *2021 IEEE International Conference on Blockchain (Blockchain)*, 347–352. <https://doi.org/10.1109/Blockchain53845.2021.00055>
- Alabdulkarim, Y., Alameer, A., Almukaynizi, M., & Almaslukh, A. (2021). SPIN: A Blockchain-Based Framework for Sharing COVID-19 Pandemic Information across Nations. *Applied Sciences, 11(18)*, 8767. <https://doi.org/10.3390/app11188767>
- Bansal, A., Garg, C., & Padappayil, R. P. (2020). Optimizing the Implementation of COVID-19 “Immunity Certificates” Using Blockchain. *Journal of Medical Systems, 44(9)*, 140. <https://doi.org/10.1007/s10916-020-01616-4>
- Barati, M., Buchanan, W. J., Lo, O., & Rana, O. (2021). A privacy-preserving distributed platform for COVID-19 vaccine passports. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3492323.3495626>
- Cao, Y., Chen, J., & Cao, Y. (2022). Blockchain-Based Privacy-Preserving Vaccine Passport System. *Security and Communication Networks, 2022*, 1–16. <https://doi.org/10.1155/2022/4769187>
- Chaudhari, S., Clear, M., Bradish, P., & Tewari, H. (2021). Framework for a DLT Based COVID-19 Passport. *Lecture Notes in Networks and Systems, 285(13)*, 108–123. [https://doi.org/10.1007/978-3-030-80129-8\\_9](https://doi.org/10.1007/978-3-030-80129-8_9)
- Constantinos Marios Angelopoulos, A. D. and V. K. (2020). DHP Framework: Digital Health Passports Using Blockchain. *Monthly Notices of the Royal Astronomical Society, 359(2)*, 567–579. <https://doi.org/10.1111/j.1365-2966.2005.08922.x>
- Deka, S. K., Goswami, S., & Anand, A. (2020). A blockchain based technique for storing vaccination records. *2020 IEEE Bombay Section Signature Conference, IBSSC 2020*, 135–139. <https://doi.org/10.1109/IBSSC51096.2020.9332171>
- Dima, S. M., Hasikos, A., Kampakis, S., Mourouzis, T., & Papageorgiou, A. (2021). *Hygiea: A secure, smart, privacy-preserving and interoperable Blockchain solution for the Covid-19 pandemic*. 1–18. <https://doi.org/https://doi.org/10.48550/arXiv.2107.09926>
- Eisenstadt, M., Ramachandran, M., Chowdhury, N., Third, A., & Domingue, J. (2020). COVID-19 Antibody Test/Vaccination Certification: There’s an App for That. *IEEE Open Journal of Engineering in Medicine and Biology, 1*, 148–155. <https://doi.org/10.1109/OJEMB.2020.2999214>
- Ethereum-Oficial. (2022). *Ethereum*. <https://ethereum.org/en/>
- Gruener, D. (2020). Immunity Certificates : If We Must Have Them , We Must Do It Right. *Safra Centre for Ethics*.
- Hasan, H. R., Salah, K., Jayaraman, R., Arshad, J., Yaqoob, I., Omar, M., & Ellahham, S. (2020). Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates. *IEEE Access, 8*, 222093–222108. <https://doi.org/10.1109/ACCESS.2020.3043350>
- Hernández-Ramos, J. L., Karopoulos, G., Geneiatakis, D., Martin, T., Kambourakis, G., & Fovino, I. N. (2021). Sharing Pandemic Vaccination Certificates through Blockchain: Case Study and Performance Evaluation. *Wireless Communications and Mobile Computing, 2021*, 1–12. <https://doi.org/10.1155/2021/2427896>
- Hicks, C., Butler, D., Maple, C., & Crowcroft, J. (2020). *SecureABC: Secure AntiBody Certificates for*

- COVID-19. <https://doi.org/https://doi.org/10.48550/arXiv.2005.11833>
- Hyperledger-Fundation. (2022). *Hyperledger*. Fundation
- INMUNITY. (n.d.). *A simple and secure certificate of covid-19 immunity*. 2021. Retrieved May 1, 2022, from <https://www.immupass.org/>
- Ishengoma, F. (2021). NFC-Blockchain Based COVID-19 Immunity Certificate: Proposed System and Emerging Issues. *Information Technology and Management Science*, 24(December 2021), 26–32. <https://doi.org/10.7250/itms-2021-0004>
- Java-Netbeans. (2022). *Java*. <https://netbeans.apache.org/kb/docs/java/index.html>
- Karopoulos, G., Hernandez-Ramos, J. L., Kouliaridis, V., & Kambourakis, G. (2021). A Survey on Digital Certificates Approaches for the COVID-19 Pandemic. *IEEE Access*, 9, 138003–138025. <https://doi.org/10.1109/ACCESS.2021.3117781>
- Khan, D., Hashmani, M. A., Jung, L. T., & Junejo, A. Z. (2022). Blockchain Enabled Track-and-Trace Framework for Covid-19 Immunity Certificate. *2022 2nd International Conference on Computing and Information Technology (ICCIIT)*, 248–253. <https://doi.org/10.1109/ICCIIT52419.2022.9711597>
- Lemmon, A. (2021). Re-shaping the future of identity through user-owned verifiable credentials. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–2. <https://doi.org/10.1109/ICBC51069.2021.9461078>
- Madhwal, Y., Yanovich, Y., & Chumakov, I. (2021). CoVID-19 Vaccination Certificate Supply Verification Based on Blockchain. *ACM International Conference Proceeding Series*, 88–93. <https://doi.org/10.1145/3510487.3510500>
- Mithani, S. S., Bota, A. B., Zhu, D. T., & Wilson, K. (2022). A scoping review of global vaccine certificate solutions for COVID-19. *Human Vaccines and Immunotherapeutics*, 18(1), 1–12. <https://doi.org/10.1080/21645515.2021.1969849>
- MSP. (2022). *SOLICITUD CERTIFICADO DE VACUNACIÓN MSP ECUADOR*. Ministerio de Salud Pública de Ecuador.
- Shamsi, K., Khorasani, K. E., & Shayegan, M. J. (2020). *A Secure and Efficient Approach for Issuing KYC Token As COVID-19 Health Certificate Based on Stellar Blockchain Network*. <https://doi.org/10.22133/IJWR.2020.250275.1070>
- Ubuntu-Desktop. (2022). *Ubuntu Desktop*. <https://ubuntu.com/download/desktop>
- Ubuntu-Server. (2022). *Sistema Operativo Ubuntu*. <https://ubuntu.com/download/server>
- Wang, S., Li, Q., Hou, J., & Jiang, J. (2020). Security control components for epidemic prevention donation management blockchain. *BSCI 2020 - Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, Co-Located with AsiaCCS 2020, January*, 73–84. <https://doi.org/10.1145/3384943.3409424>
- Wu, H., Shang, Y., Wang, L., Shi, L., Jiang, K., & Dong, J. (2019). A patient-centric interoperable framework for health information exchange via blockchain. *ACM International Conference Proceeding Series*, 76–80. <https://doi.org/10.1145/3376044.3376055>