UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

MODELO DE CONEXIÓN Y DATOS PARA EL SEGUIMIENTO DE PACIENTES DE HOSPITALES EN ECUADOR BASADO EN IOT Y BLOCKCHAIN

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

AUTOR: GALO NICOLAS CRUZ CALERO

TUTOR: JOE FRAND LLERENA IZQUIERDO

Guayaquil – Ecuador

2022

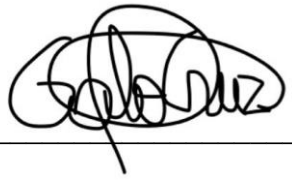
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Galo Nicolas Cruz Calero con documento de identificación N° 0930091434 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, 7 de Febrero del año 2022

Atentamente,



Galo Nicolas Cruz Calero
C.I.: 0930091434

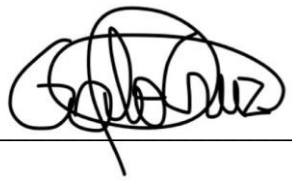
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Galo Nicolas Cruz Calero con documento de identificación No. 0930091434, 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 del Artículo Académico: "Modelo de conexión y datos para el seguimiento de pacientes de hospitales en Ecuador basado en IoT y 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, 7 de Febrero del año 2022

Atentamente,



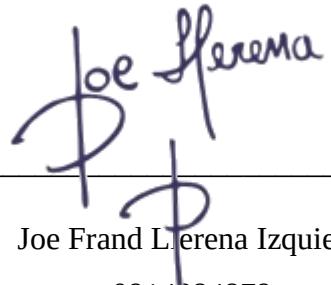
Galo Nicolas Cruz Calero
C.I.: 0930091434

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: Modelo de conexión y datos para el seguimiento de pacientes de hospitales en ecuador basado en IoT y Blockchain, realizado por Galo Nicolas Cruz Calero con documento de identificación N° 0930091434, 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, 7 de Febrero del año 2022

Atentamente,



Joe Frand Llerena Izquierdo
0914884879

DEDICATORIA

Dedico esta Tesis a Mis Padres, el Ing. Darwin Cruz Velasco y Lic. María Elena Calero De Cruz, por su dedicación y entrega su esfuerzo a lo largo de mi carrera, su apoyo incondicional en cada instante de mi formación académica, también hago extensivo esta dedicatoria a mis Docentes en los cuales siempre encontré la orientación y enseñanzas oportunas la luz de mis conocimientos y por último y no menos importantes a mis compañeros y futuros colegas, amigos solidarios y hermanos de la vida.

AGRADECIMIENTO

Agradezco a Dios Creador de la VIDA, a mis Abuelos Sr. Nicolás Cruz Merelo y Sra. Laura Velasco de Cruz. Gracias a ellos en toda mi formación desde mis inicios escolares hasta ver culminar mi carrera hoy como Ingeniero en Sistemas, mis hermanos Carlos, Darwin y María Elena, por su apoyo y afecto demostrándome la fuerza que tiene el AMOR.

RESUMEN

El uso de la tecnología para dar el seguimiento en línea a los signos de salud de una persona es una idea muy innovadora, especialmente en este tiempo que se vive en pandemia. Además de ser eficiente, por tener valores en tiempo real, es necesario mantener su privacidad y seguridad, en un entorno cada vez más público. El objetivo de esta investigación es determinar un modelo de conexión y de datos para el seguimiento de pacientes de hospitales en Ecuador basado en IoT y Blockchain. La metodología de este trabajo es una investigación analítica descriptiva de enfoque cuantitativo cuasi experimental. Se aplica la técnica de revisión de literatura para el análisis correspondiente y determinar los factores viables aplicables a un modelo computacional en el contexto ecuatoriano. Este estudio propone un modelo de 6 niveles con sus participantes, funciones y estructura de datos. Los resultados evidencian que el 19% de las investigaciones analizadas permiten un enfoque al seguimiento del COVID-19 mediante la tecnología Blockchain y un 52% son viables para corroborar aplicabilidad del modelo propuesto al contexto ecuatoriano. Se concluye que la tecnología Blockchain capta la aceptación de investigadores en varios ámbitos de estudio debido a que permite mantener la información en forma descentralizada y segura, aplicable a modelos según diversos contextos, así como su arquitectura computacional es un excelente complemento para IoT.

Palabras claves: Blockchain, Internet de las cosas, Salud, Seguridad, COVID-19.

ABSTRACT

The use of technology to monitor a person's health signs online is a very innovative idea, especially in this time of a pandemic. In addition to being efficient, by having values in real time, it is necessary to maintain your privacy and security, in an increasingly public environment. The objective of this research is to determine a connection and data model for monitoring hospital patients in Ecuador based on IoT and Blockchain. The methodology of this work is a descriptive analytical research with a quasi-experimental quantitative approach. The literature review technique is applied for the corresponding analysis and to determine the viable factors applicable to a computational model in the Ecuadorian context. This study proposes a 6-level model with its participants, functions and data structure. The results show that 19% of the analyzed investigations allow an approach to monitoring COVID-19 through Blockchain technology and 52% are viable to corroborate the applicability of the proposed model to the Ecuadorian context. It is concluded that Blockchain technology captures the acceptance of researchers in various fields of study because it allows information to be maintained in a decentralized and secure manner, applicable to models according to various contexts, as well as its computational architecture is an excellent complement for IoT.

Key words: Blockchain, Internet of Things, Healthcare, Security, COVID-19.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

Es de conocimiento público que el efecto de la pandemia del COVID-19 en el año 2020 ha afectado la salud de muchas personas (Apuzzo & Kirkpatrick, 2020)(Al-Kumaim et al., 2021). El manejo de los datos de los pacientes en muchos países evidenció una carencia de confidencialidad, integridad y disponibilidad de la información (Khalil et al., 2022)(Wolkewitz & Puljak, 2020), por esta razón la seguridad durante el proceso de captura de datos y almacenamiento de registros médicos es un permanente desafío (Primahendra et al., 2020)(Majeed, 2021)(Zhang et al., 2022), y varios países adoptaron redes IoT para detectar lugares de posible infección, pero algunos datos perdieron su seguridad e integridad (Mallikarjuna et al., 2021)(Adamy & Rani, 2022)(McBroome et al., 2022).

Internet of Things (IoT) obtiene gran cantidad de datos, y brinda muchos servicios en sectores de transporte, redes, ciudades y salud, los datos del sector salud son muy sensibles y críticos, además se utiliza IoT para seguimiento de pacientes mediante sensores que detectan y envían los datos a internet (Aujla & Jindal, 2021). Blockchain (BkC) es una tecnología que aumenta la seguridad y privacidad en dominios IoT, con esta tecnología los datos de salud se guardan en bloques inmutables que mantienen la integridad de información, la descentralización de BkC no permite intermediarios y los registros de salud pueden ser datos estructurados y no estructurados (Ray, Chowhan, et al., 2021)(Melendrez-Caicedo & Llerena-Izquierdo, 2022).

En BkC las solicitudes de almacenamiento en datos descentralizadas van en aumento y son confiables como transacciones en una infraestructura IoT que permiten una interoperabilidad estándar (Abou-Nassar et al., 2020), además BkC se integra en dominios IoT como: hogares, ciudades, salud (Ray, Chowhan, et al., 2021), negocios de Pymes, industria automotriz y cadena de suministros (Karthikeyyan et al., 2019).

BkC e IoT son tecnologías diferentes, pero la combinación de estas “es un cambio de paradigma masivo” porque incentiva el progreso en los sistemas de salud en que BkC afronta las vulnerabilidades de IoT y soluciona los inconvenientes de seguridad en la conexión de dispositivos IoT (Firouzi & Farahani, 2021); los datos que toman los sensores IoT son: latidos de corazón, presión, temperatura, glucosa (Aujla & Jindal, 2021), pulso, electrocardiograma, electromiografía, respuesta de piel (Ray, Chowhan, et al., 2021), actividad eléctrica del cerebro, volumen de órganos, posicionamiento, altímetro, respiración y gas (Firouzi & Farahani, 2021).

Por ejemplo en Perú, por motivos de fraude en compras y alteración de la información de medicamentos que afecta la prestación de servicios de salud, se utiliza un modelo Cloud para la gestión de compras mediante la combinación BkC e IoT (Celiz et al., 2019); en Corea del Sur se utiliza esta combinación para seguir el movimiento de los infectados de Covid-19 mediante IoT y los datos se almacenan en una nube BkC (Firouzi & Farahani, 2021). En Ecuador es posible adoptar esta combinación Blockchain e IoT para seguimiento (en sitio o remoto) de pacientes porque los dispositivos IoT son más económicos, los hospitales públicos/privados tienen acceso a internet, los espacios en la nube son más accesibles, los doctores/pacientes/proveedores tienen internet en sus dispositivos móviles, y existen plataformas BkC que son código libre. De acuerdo a la investigación exploratoria en este estudio, existen propuestas de BkC en área de salud y propuestas de IoT en forma independiente cada uno; en Ecuador se evidencia una investigación (Pérez-Ch et al., 2021) que propone la combinación BkC e IoT para seguimiento de pacientes, los demás trabajos pertenecen a otros países (Sánchez Guzmán, 2021)(Guaigua Bucheli, 2021)(Terán Terranova, 2021).

Los argumentos, basados en artículos científicos, justifican la presente propuesta, prever conectividad de los datos que pertenecen a pacientes, provenientes de los sensores IoT hacia las entidades de salud, conservando la seguridad y privacidad (Aujla & Jindal, 2021)(Ponce Larreategui, 2021); se debe garantizar el seguimiento de pacientes sin manipulaciones, almacenamiento seguro de datos, manteniendo la integridad de datos y autenticación del paciente (Morán Maldonado, 2021).

BkC es una excelente solución para proteger los registros de salud en dominios IoT (Ray, Chowhan, et al., 2021)(Guaman Villalta, 2021)(Aguirre Sánchez, 2021)(Chévez Morán, 2021)(Salazar, 2018), la combinación de BkC e IoT permite la asistencia en el diagnóstico y detección de enfermedades en situaciones de pandemia, aumenta la confianza en datos de atención médica e intercambio entre pacientes y doctores (Mallikarjuna et al., 2021)(Muñoz Campuzano, 2021), además el monitoreo, intercambio de datos y trazabilidad son confiables (Alam et al., 2021)(Miranda Jiménez, 2021); las infraestructuras ascendentes aseguran la adición de nodos y BkC proporciona un entorno para implementar una infraestructura IoT que sea más confiable y eficiente (Abou-Nassar et al., 2020)(Llerena Izquierdo et al., 2009)(Llerena Izquierdo et al., 2018).

En esta investigación se propone diseñar un modelo para seguimiento remoto de pacientes que pertenecen a un hospital, este modelo utiliza las características y beneficios de las tecnologías BkC e IoT. El objetivo de esta investigación es determinar un modelo de conexión y datos para el seguimiento de pacientes de hospitales en Ecuador basado en IoT y Blockchain.

Además, se da a conocer sobre los conceptos de BkC, IoT, los beneficios de utilizar estas tecnologías combinadas y la utilización de estas tecnologías; nuestra contribución está en la fase resultados: Identificación de los diferentes modelos, esquemas y arquitecturas para procesos de conexión y envío de datos, un modelo de conexión y datos para el seguimiento de pacientes, y evaluación de factores viables del modelo aplicable a hospitales en el contexto ecuatoriano. Finalmente se presentan las discusiones y conclusiones.

2. METODOLOGÍA

Este trabajo es una investigación analítica-descriptiva de enfoque cuantitativo cuasi experimental. El alcance exploratorio en su fase inicial permite analizar los modelos, esquemas o arquitecturas de los artículos científicos relevantes seleccionados de las bases IEEE Xplore, Scopus, Springer, ACM entre otras que aplican la combinación BkC e IoT en el área de salud y permiten proponer el desarrollo de un modelo adecuado al contexto del estudio.

El modelo descrito se encuentra formado por niveles/capas, sensores médicos IoT, conexiones, plataforma blockchain, servicios en la nube y aplicaciones informáticas. Durante la investigación se determina la plataforma blockchain a utilizar (pública o privada), además de los actores con sus responsabilidades; se describen las funciones del Smart Contract; se determina la estructura de datos que debe almacenarse en la plataforma blockchain. Finalmente se forma la tabla de factores viables del modelo validando los elementos fundamentales que pueden incidir para aplicar el modelo en el contexto del país.

2.1. Conceptos básicos de Blockchain

Blockchain (BkC) es una lista de registros en bloques que están enlazados y encriptados, para la lista un interesado inicia una transacción y se crea el bloque, luego la transacción es autorizada por los interesados para que el bloque se adicione a la cadena, el bloque es único y distribuido en la red (Ray, Dash, et al., 2021); otro autor considera que BkC es un conjunto de datos escalable de acuerdo a los nodos y los nuevos datos se adicionan a la cadena (Abou-Nassar et al., 2020).

Existen cuatro tipos de BkC: a) público, b) privado, c) consorcio y d) híbrido; el tipo público permite a cualquiera usuario ingresar a los bloques de datos; en el tipo privado se necesita permisos para acceder; en el tipo consorcio un grupo de interesados otorga o revoca el acceso a los bloques de datos (Ray, Chowhan, et al., 2021); el tipo híbrido es una combinación de público y privado, el usuario otorga permisos o libre acceso (Ray, Dash, et al., 2021).

Existen varias plataformas BkC para su utilidad en salud, las más adecuadas para dominios IoT son estudiadas en (Ray, Dash, et al., 2021); entre las plataformas públicas se tiene a Ethereum, Bitcoin, Ripple y Stellar, entre las plataformas privadas se tiene a Quorum, Hyperledger Sawtooth, Hyperledger Fabric, Hyperledger Iroha, Neo y Medicalchain.

2.2. Beneficios de utilizar la combinación Blockchain e IoT en salud

Un beneficio determinado de esta tecnología es la interoperabilidad para intercambio de datos entre los nodos de la red IoT ya que esto reducen costos en sistemas informáticos, los nodos aumentan la confidencialidad y disponibilidad de los datos; en el caso de la atención médica inmediata permite a los dispositivos IoT utilizar las comunicaciones de altas prestaciones así los datos capturados de los pacientes se mantienen inmutables y los pacientes pueden observar los procesos porque son transparentes y genuinos (Ray, Chowhan, et al., 2021).

Otros beneficios son la optimización de la interoperabilidad, el almacenamiento distribuido, la autenticación de interesados, la confiabilidad en la información, la seguridad de mantener los datos inmutables, mejorar interacciones entre pacientes, doctores, y proveedores de servicios médicos; finalmente los interesados de esta tecnología pueden aumentar la eficiencia de la red al usar IoT, además los datos mantienen su integridad y confidencialidad (Abou-Nassar et al., 2020), y la descentralización se convierte en fiable y segura entre los intermediarios (Garg et al., 2020).

2.3. Uso de la combinación Blockchain e IoT en salud

En el diseño del *framework* en BkC la confiabilidad de los datos es un elemento primordial, ya que brindar accesos y compartir datos entre pacientes, doctores y casas de salud en un contexto público o privado debe ser una ventaja resultante para ser incluida en esta propuesta.

La información está en una nube IoT que toma datos de la casa del paciente, el framework los recepta y los datos pasan por una estructura computacional que está formado por tres niveles: sensores, registro de salud y usuarios (Mallikarjuna et al., 2021). Los datos son transmitidos de forma eficiente por medio de los sensores IoT, y son enviados a BkC para preservar la seguridad, las tres capas del modelo son representadas por escenario IoT, escenario blockchain y la nube de alojamiento (Aujla & Jindal, 2021).

Se propone un esquema para asegurar la transmisión y privacidad de los registros de salud, en este esquema los datos son compartidos solo a interesados, los doctores envían medicación y diagnósticos, así los datos generados por los sensores son heterogéneos y el esquema queda conformado por los tres niveles (Ray, Chowhan, et al., 2021).

Para aumentar la interoperabilidad y seguridad en la salud, es aceptable un framework formado de cuatro niveles, el primero conformados por los sensores y actuadores, en el segundo nivel se

establece la red pública blockchain Ethereum, el tercer nivel se conforma por el protocolo de salud establecido que contiene la estructura de los datos, en el cuarto nivel están los servicios informáticos en la nube (Abou-Nassar et al., 2020).

El *modelo* reduce los fraudes de compras, reduce las alteraciones de la información, mejora la visibilidad y trazabilidad para garantizar la calidad de los medicamentos, y se accede desde una aplicación web (Celiz et al., 2019).

BkC garantiza la integridad de los datos a través de su almacenamiento descentralizado para una mayor seguridad, en este entorno para poder alterar la información almacenada, se debe modificar la información en el 51% de computadoras distribuidas en la red; las redes IoT están basadas en los modelos cliente-servidor y se conectan a servidores en la nube, BkC permite disminuir costos en recursos gracias a que establece una red peer-to-peer (Ray, Dash, et al., 2021).

El uso de BkC para almacenar datos y para la recuperación de los mismos garantiza conservar la privacidad de la información y tener control sobre la información almacenada, además está enfocado en la confianza para brindar una mejor atención de salud; con la pandemia de covid-19 los pacientes no desean hacer público su estado de salud y esto permite proteger su información (Garg et al., 2020).

La *arquitectura* recopila datos de pacientes con diabetes y se comparten con los doctores, en esta arquitectura los pacientes permiten el acceso a sus datos y se estabiliza la integridad y privacidad, además está formada por cuatro niveles: dispositivos, equipo de doctores, blockchain Ethereum y smart contract (ver Fig. 1) (Azbeg et al., 2018).

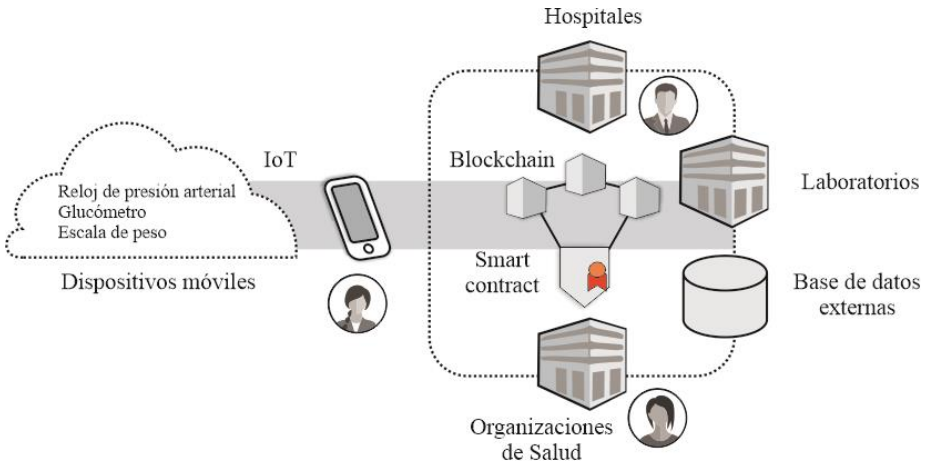


Figura 1. Arquitectura que aplica Blockchain e IoT

La tecnología en el sector de salud ofrece beneficios como el IoT que permite tener un control remoto de la salud y usar la atención médica inteligente para brindar una atención más cuidadosa, con IoT se aplican sensores montados en el lado del paciente y detectan los parámetros de salud; estos datos son enviados a un servidor médico y se almacenan en una base de datos, esto permite al médico monitorear su paciente en tiempo real (Xiang et al., 2020).

Un gran desafío es la interoperabilidad de datos, en este caso un paciente de un centro de salud es asignado a otro centro y se solicita la información; con el uso de una arquitectura BkC e IoT se brinda una solución para mantener seguridad y privacidad de la información, este avance tecnológico permite mejorar los procesos y análisis de datos sobre pacientes crónicos que requieren atención médica urgente (Alamri et al., 2021).

El objetivo de BkC es permitir el intercambio de información entre proveedores de salud garantizando en todo momento la integridad, protección y privacidad de los datos, además el uso de IoT permite el manejo de grandes cantidades de tráfico en BkC y esto soluciona los problemas de escalabilidad de grandes poblaciones de pacientes; adicionalmente para corroborar la validez de la información se trabaja con un auditor externo de confianza que se encarga de validar la información compartida y evitar contenido digital fraudulento (Jabbar et al., 2020).

En la arquitectura de alto nivel, se propuso capturar los datos con dispositivos médicos IoT y estos datos almacenarse en una plataforma pública BkC para dar seguridad y privacidad a los datos de pacientes, en esta arquitectura los datos pasan del dispositivo IoT a través de red inalámbrica, red alámbrica o bluetooth (Rahman et al., 2020).

3. RESULTADOS

3.1. Identificar los diferentes modelos, esquemas y arquitecturas para procesos de conexión y envío de datos.

Se revisan y tabulan varios artículos científicos de las bibliotecas virtuales indexadas, luego del análisis para determinar los modelos, esquemas y arquitecturas que sirven de insumo para el diseño del modelo, se obtienen 27 artículos de relevancia, en la Tabla 1 se presentan los artículos seleccionados de los últimos tres años y relacionados en la utilización de ambas tecnologías BkC e IoT en salud.

Tabla 1. Artículos científicos de BkC e IoT en salud

Tipo	Art	Objetivo principal	Funciones de BkC	Funciones IoT
Sistemas	(Pérez-Ch et al., 2021)	Alerta de salud	Trazabilidad de brotes, privacidad, seguridad	Envío de datos
	(Bhattacharya et al., 2020)	Monitoreo de salud	Rendimiento y seguridad	Recolectar datos
	(Ramane et al., 2021)	Monitoreo de salud	Seguridad	Recolectar datos
	(Juyal et al., 2020)	Monitoreo de piel	Seguridad, Privacidad de datos	Comunicar datos
Framework	(Mallikarjuna et al., 2021)	Disminuir tiempo respuesta	Escalabilidad y confiabilidad de datos	Recolectar datos
	(Abou-Nassar et al., 2020)	Interoperabilidad descentralizada	Autenticación, confidencialidad	Comunicar datos
	(Ray, Dash, et al., 2021)	Almacenamiento descentralizado	Seguridad, Transparencia	Recolectar datos
	(Rahman et al., 2020)	Control de síntomas y diagnostico	Privacidad y anonimato de datos	Comunicar datos
Modelo	(Aujla & Jindal, 2021)	Monitoreo de salud	Seguridad, Privacidad de datos	Comunicar datos
	(Karthikeyyan et al., 2019)	General	Seguridad	Recolectar datos
	(Celiz et al., 2019)	Reducir fraude de medicina	Trazabilidad, compartir datos	Estado de las medicinas
	(Garg et al., 2020)	Notificación de casos enfermos	Confianza, Privacidad de datos	Comunicar datos
	(Xiang et al., 2020)	Biometría personal	Seguridad, Privacidad de datos	Captura biométrica
	(Dwivedi et al., 2019)	Alerta de salud	Seguridad, Privacidad de datos	Comunicar datos
	(Srivastava et al., 2019)	Monitoreo de pacientes	Seguridad, Privacidad de datos	Comunicar datos
	(Saha et al., 2020)	Control de acceso	Seguridad, Funcionalidad	Recolectar datos
Arquitectura	(Ray, Chowhan, et al., 2021)	Gestión del flujo de datos	Privacidad de datos	Envío de datos
	(Azbeg et al., 2018)	Seguimiento de diabetes	Seguridad, Privacidad de datos	Recolectar datos

	(Alamri et al., 2021)	Interoperabilidad entre sistemas	Privacidad de datos	Recolectar datos
	(Jabbar et al., 2020)	Intercambio de información	Integridad, protección y privacidad de los datos	Recolectar datos
	(Kaschel & Diaz, 2021)	Monitoreo de salud	Seguridad, Privacidad de datos	Comunicar datos
	(A et al., 2021)	Monitoreo de alimentación	Seguridad	Recolectar datos
	(Hewa et al., 2020)	Telemedicina	Autenticación, integridad y privacidad de datos	Comunicar datos
	(Rakib et al., 2021)	Monitoreo de salud	Seguridad, Privacidad de datos	Captura biométrica
	(AlJemy et al., 2019)	General	Seguridad	Recolectar datos
	(Fernández-Caramés et al., 2019)	Seguimiento de diabetes	Intercambio seguro de datos, privacidad	Comunicar datos
	(Tahir et al., 2020)	Monitoreo de pacientes	Intercambio seguro de datos, Seguridad, Inmutabilidad	Recolectar datos

Fuente: Elaboración propia.

Los artículos se clasifican en 4 categorías como: Arquitectura 40%, Modelo 30%, Sistema 15%, Framework 15%, esto significa que cada propuesta en su contenido especifica un tipo de solución en el ámbito de salud (ver Fig. 2).

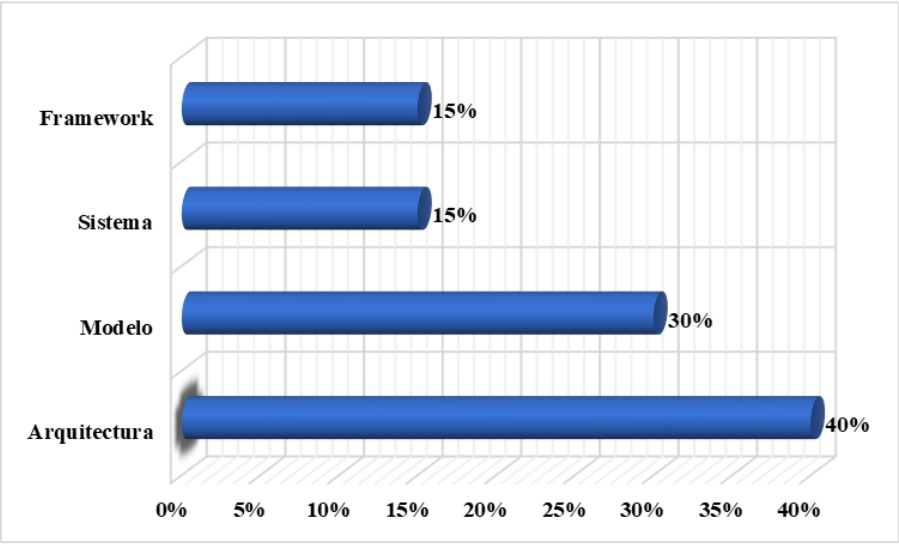


Figura 2. Porcentaje de investigaciones de acuerdo con la categorización establecida

Cada artículo tiene su propio objetivo principal, el más común es Monitoreo en Salud en 33% de los artículos, los objetivos: Alerta de salud, Interoperabilidad y Seguimiento de diabetes se nombran en 7% de los artículos cada uno, los demás objetivos se nombran una sola vez 46% (ver Fig. 3).

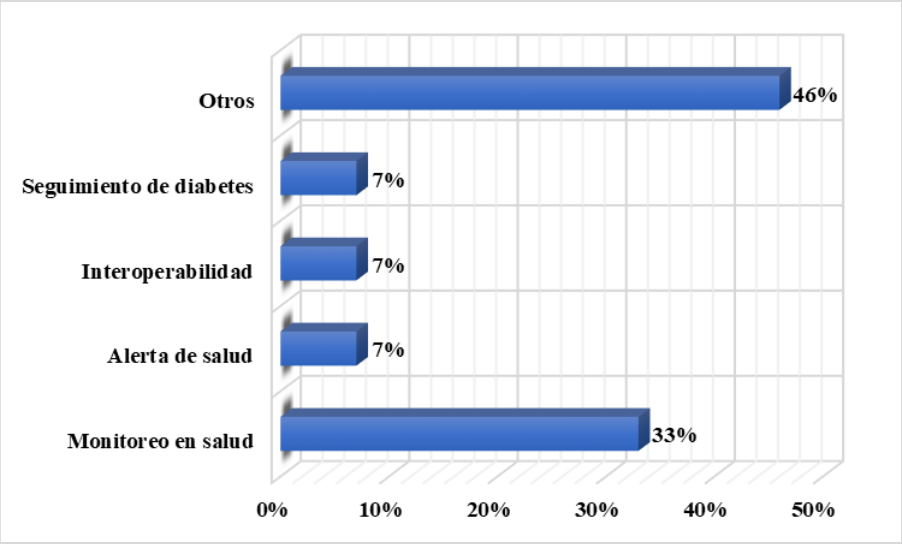


Figura 3. Porcentaje de trabajos de investigación en BkC e IoT de acuerdo con los objetivos

En las funciones de BkC, el más aspecto más común es la Seguridad, en 17 artículos, la Privacidad en 16 artículos, las funciones: Intercambio, Integridad, Confianza y Autenticación se nombran 2 veces, las demás funciones se nombran una sola vez (ver Fig. 4).

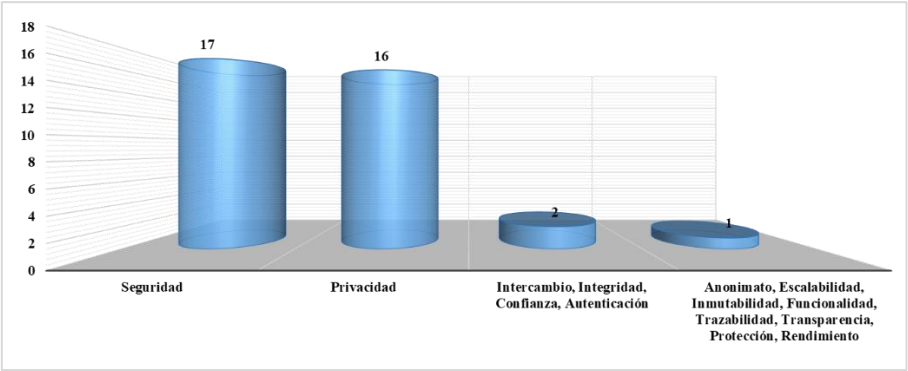


Figura 4. Funciones de BkC

En las funciones de IoT, el factor más común es Recolectar datos porque los dispositivos solo recopilan datos del entorno y otros dispositivos de comunicación se encargan de pasarlos a internet; Comunicar datos es la función de recolección y envío de los datos al internet; Envío de datos es solo paso de datos al internet; otros sistemas se basan sólo en captura de datos biométricos y un artículo se especializa en información de las medicinas (ver Fig. 5).

La seguridad, privacidad, recolección y comunicación de datos son las funciones más utilizadas por las propuestas BkC e IoT en salud.

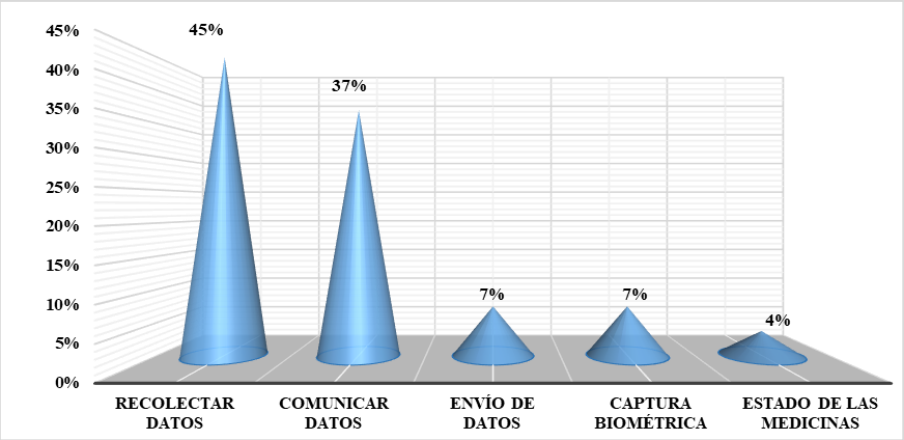


Figura 5. Funciones de IoT

3.2. Establecer un modelo de conexión y datos para el seguimiento de pacientes de hospitales en Ecuador basado en Blockchain e IoT

Se propone un modelo de alto nivel y generalizado que conecte dispositivos IoT médicos enlazados a pacientes de hospitales, y los doctores u hospital puedan realizar el seguimiento de los signos vitales o críticos (ver Fig. 6).

1.- Nivel Usuarios. En este nivel están los pacientes, los doctores, los hospitales, las instituciones de gobierno como ministerio de salud, y otros interesados como proveedores de salud privados o compañías de seguro o laboratorios externos. En el caso de acceso para Otros interesados, los pacientes deben solicitar al hospital se brinde el permiso y acceso para terceros hacia sus datos. La responsabilidad del paciente es mantenerse conectado y reportar novedades con respecto a los dispositivos; la responsabilidad de los doctores y enfermeras es atender las alertas del sistema y comunicarse con el paciente; el personal de los hospitales realiza el registro de los pacientes, doctores y enfermeras; las enfermeras registran las citas, examen clínico, medicación, los bodegueros realizan la gestión de las medicinas; la responsabilidad de las instituciones de gobierno es velar por la operatividad íntegra de la red BkC; la responsabilidad de otros interesados se propone sea solo de lectura de los datos de los pacientes.

2.- Nivel Dispositivos IoT Médicos. Este nivel captura los datos del paciente a través de sensores médicos, y los datos que se capturan son el nombre del sensor, unidad de medida, valor y hora; los dispositivos IoT considerados son: temperatura corporal, acelerómetro, electrocardiogramas, giroscopio, magnetómetro, frecuencia del pulso, saturación de oxígeno, respuesta galvánica de la piel y glucosa en sangre; los dispositivos pueden utilizar wifi,

bluetooth, radio frecuencia u otra vía. Se contempla mantener la seguridad de los dispositivos IoT con sus mismos protocolos de comunicación y actualización continua del firmware.

3.- Nivel Comunicación. Si el paciente está en casa, los dispositivos de comunicación son captadores de onda corta, captadores de radio frecuencia, router inalámbrico, switch y la red del proveedor de internet; si el paciente está fuera de casa, el dispositivo de comunicación es el teléfono celular y la red del proveedor de telefonía; si el paciente está en un hospital, los dispositivos de comunicación están formados por la infraestructura propia del hospital como wifi, switch, router, redes. Aquí también se contempla mantener la seguridad de los dispositivos con sus mismos protocolos de comunicación.

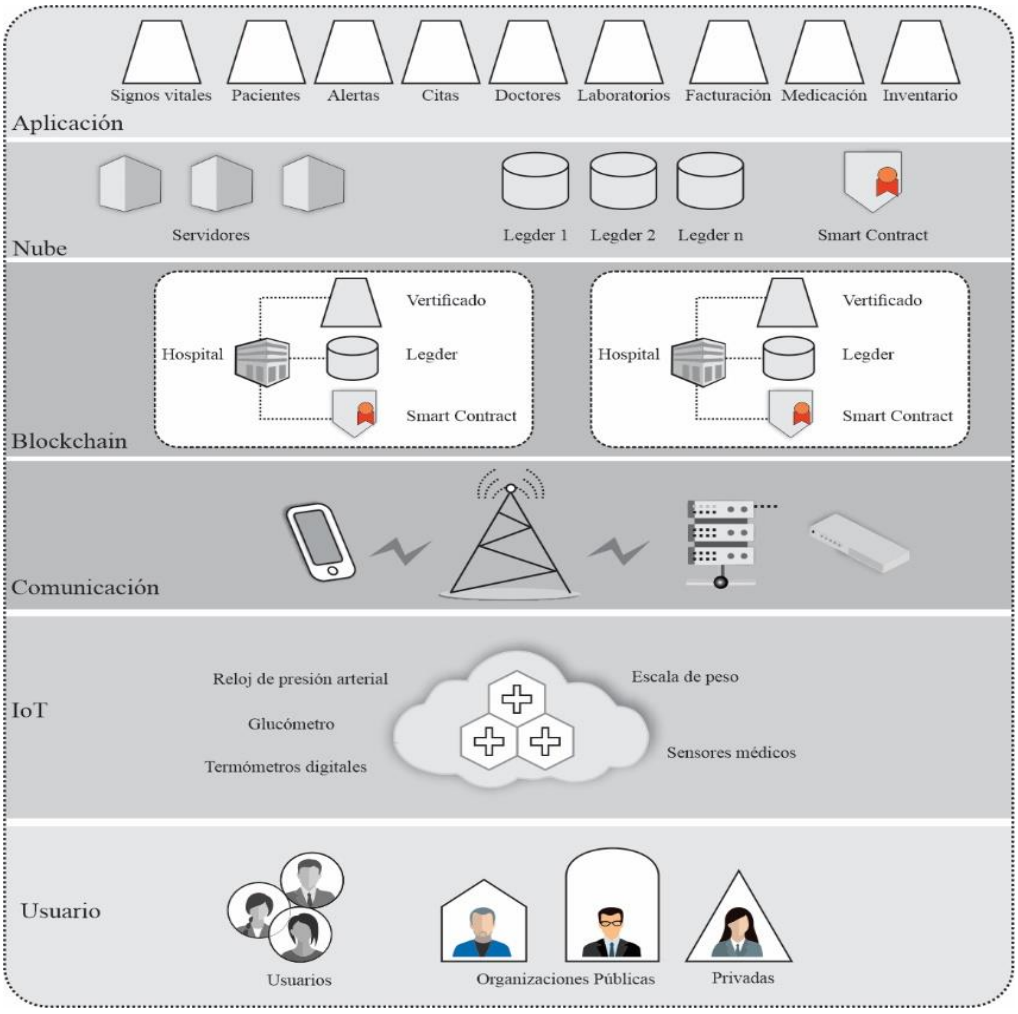


Figura 6. Modelo Blockchain e IoT.

4.- Nivel Blockchain. La red BkC es una red privada para que solo los hospitales tengan acceso autorizado a esta red y desde cualquier lugar los datos de los pacientes son entregados a los hospitales; en este nivel cada hospital es un nodo de la red BkC, la red puede empezar con dos

hospitales y se pueden adicionar más hospitales por la escalabilidad que es característica de BkC; los datos personales de los pacientes son registrados por el hospital y replicados a todos los ledger de los hospitales; si el paciente se encuentra en el hospital los datos de salud son recolectados en su propia red, o si el paciente se encuentra en casa/calle los datos de salud son capturados por las redes de comunicación y los datos son enviados al nodo-hospital; además en cada nodo-hospital se activan las alarmas por emergencias, se registra información de pacientes, autorizan y aprueban las nuevas transacciones generadas por los pacientes, en este nivel existe un consenso entre los nodos-hospitales, cada nodo contiene sólo una copia declarativa del ledger y una copia del Smart contract y su certificado de autenticidad; los datos o transacciones del ledger son enviados a la nube, es decir los datos o transacciones del ledger no están en el hospital sino en la nube.

El *Smart Contract* define las funciones y políticas de acceso y alertas sobre los datos obtenidos desde los dispositivos IoT, por ejemplo una función que emita alerta al obtener datos por debajo o por encima de los niveles bajos/altos respectivamente sobre la presión arterial de un paciente, si existen datos fuera de los rangos entonces el contrato envía un mensaje de alerta al doctor o enfermera, y los datos se siguen almacenando en la nube; los proveedores de salud pueden continuar con el seguimiento de la presión arterial en tiempo real.

Entre las funciones del Smart Contract están: registro de signos vitales, registro de pacientes, emisión de alertas, registro de citas, registro de doctores, registro de resultados del laboratorio, registro de medicación, registro de medicinas, además de las consultas de la información guardada; estas funciones pueden ser invocadas desde las aplicaciones web o móviles realizadas en lenguaje Java.

La estructura de datos que debe almacenarse en la red BkC están las siguientes entidades:

Hospital: Identificación del hospital, nombre, dirección, teléfono, número de camas, número de doctores, número de enfermeras.

Signos Vitales: Identificación del paciente, identificación del dispositivo, valor, unidad de medida, fecha, hora, estado de seguimiento, posición global X, posición global Y.

Pacientes: Identificación del paciente, cedula, nombres, apellidos, dirección, teléfono, ciudad, provincia, fecha de nacimiento, numero del seguro social, genero, profesión, nombre de familiar, teléfono del familiar.

Doctores: Identificación del doctor, cédula, nombres, apellidos, teléfono, especialidad, fecha de nacimiento.

Historial médico del paciente: Identificación del historial, identificación del paciente, identificación del doctor, fecha de entrada, fecha de alta, número de cama, fecha de asignación.

Citas médicas: Identificación de la cita, identificación del paciente, identificación del doctor, número de sala, fecha, hora.

Medicinas: Identificación de la medicina, nombre, código de barra, cantidad en stock, stock mínimo, unidad de medida, identificación del hospital.

Medicación: Identificación del paciente, identificación del doctor, identificación del hospital, fecha, hora, identificación de la medicina, cantidad, unidad de medida, recomendación del doctor.

Usuarios: Identificación del usuario, cédula, estado, fecha de inicio, fecha de inactividad, contraseña.

5.- Nivel Nube. La nube tiene grandes recursos informáticos, procesamiento y almacenamiento, además la nube contiene una copia de seguridad de las transacciones generadas por los pacientes; el modelo no genera consumo de energía porque el procesamiento de datos está en la nube y en tiempo real, y es escalable debido a que el almacenamiento está en la nube. Los datos pueden ser vistos por pacientes, médicos y terceros interesados a través de las políticas de acceso que están en el Smart Contract. El Ledger contiene todos los datos o transacciones de cada paciente, y el Ledger está en los centros de datos de la nube; se considera que los nodos-hospitales tienen almacenamiento limitado y el nodo-hospital valida las transacciones mediante el consenso, luego de validar la transacción se adiciona al ledger de la nube, además el procesamiento es más veloz y el ledger de cada nodo-hospital es liviano.

6.- Nivel Aplicaciones. Contiene las aplicaciones informáticas utilizadas para gestionar los datos y transacciones de los pacientes; la aplicación Paciente es para gestión de datos de cada paciente; la aplicación Signos Vitales contiene los datos históricos generados por los dispositivos IoT; la aplicación Alertas Medicas debe avisar a los doctores encargados del paciente sobre niveles bajos o altos de salud; la aplicación Personal Médico para gestión de los datos de doctores, enfermeras y auxiliares; la aplicación Inventario de Medicinas para gestión en ingresos, egresos y transferencias de las medicinas; la aplicación Citas Médicas para gestión

en asignación, consultas o eliminación de las citas; la aplicación Imágenes para gestión de las radiografías de los pacientes; la aplicación Medicación para gestión de las recetas generadas por el doctor y entregadas al paciente; la aplicación Laboratorio para registro de examen, consulta y registro de resultados de exámenes clínicos; la aplicación Facturación para conocer costos económicos del paciente.

El modelo propuesto es confiable, es escalable puede crecer sin degradar su procesamiento, mantiene la privacidad de los pacientes, es interoperable entre los distintos hospitales, mantiene el anonimato por sus controles de acceso y los datos permanecen encriptados, todo esto debido a las características inherentes de Blockchain.

Las herramientas de software que se propone son: un servidor con Ubuntu server, Hyperledger Composer que es un framework para crear la red blockchain, lenguaje Go para implementación del Smart Contract, lenguaje Java para implementación de las aplicaciones web o móviles, un espacio en la nube para el servidor de 16GB de RAM y 500MB de espacio en disco.

3.3. Evaluar la metodología de estudio mediante contrastación de trabajos previos.

Los artículos obtenidos en la Tabla 1 fueron evaluados en otras características para establecer factores viables y determinar la aplicabilidad de nuestro modelo en hospitales del Ecuador.

El 59% de los artículos propuso plataformas públicas como Ethereum Blockchain, el 36% de los artículos propuso plataformas privadas como Hyperledger Blockchain, el 5% propuso plataformas híbrida público-privada es decir utilizaron Ethereum e Hyperledger (ver Fig. 7).

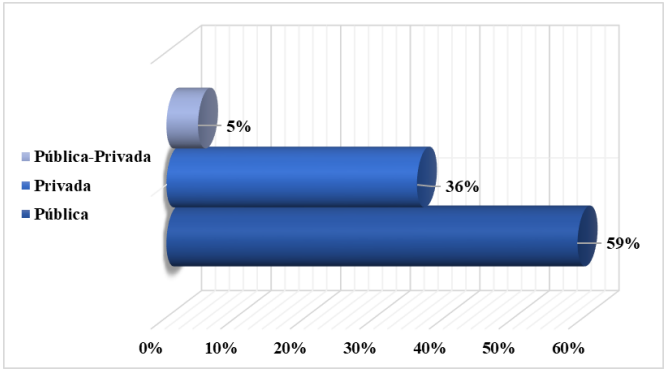


Figura 7. Porcentaje e categorización de acuerdo con plataformas

La cantidad de niveles más utilizada es de 3 niveles en 59%, la segunda y tercera más utilizadas son de 4 y 5 niveles respectivamente en 15%, la cuarta más utilizada es de 6 niveles en 7%, existe una propuesta que no está claro o no especifica en su modelo los niveles (ver Fig. 8).

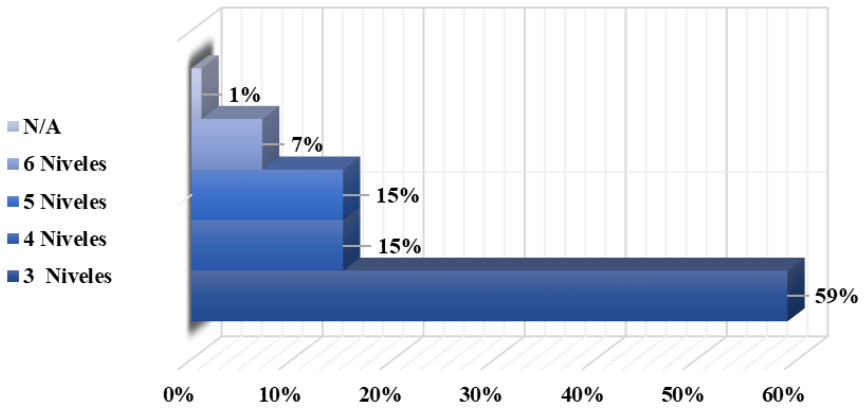


Figura 8. Porcentaje de niveles

Muchas de las propuestas nombran los niveles o capas de sus modelos, se clasificaron los nombres para visualizar la proporción en su utilización: la capa más utilizada es Blockchain en 89% aquí está incluido el ledger, Smart contract, consenso; en la segunda capa más utilizada contiene a los pacientes o usuarios en 63%; la tercera capa más utilizada contiene dispositivos o sensores o mecanismos IoT en 56%; la cuarta capa están las aplicaciones, sistemas o interfaces de presentación en 33%; la quinta capa está la nube con sus servicios en 33%; la siguiente capa está todo hardware utilizado para comunicación como switch, router u otros en 26%; la siguiente capa están los proveedores de salud como hospitales, centros privados o doctores en 11%; la capa de datos es utilizada en 11% (ver Fig. 9).

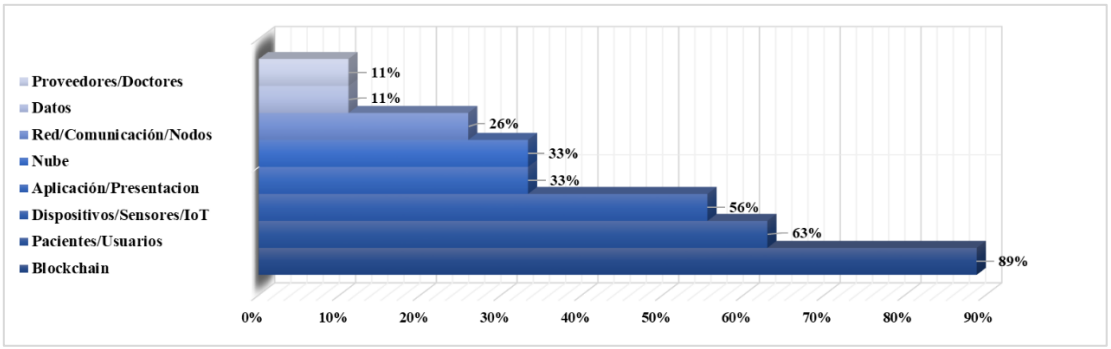


Figura 9. Porcentaje de proveedores

Además de utilizar Sensores médicos IoT, algunos artículos presentan en su propuesta la utilización de teléfono celular inteligente, raspberry y otra clase de sensores para enviar los datos de salud a la nube (ver Fig. 10).

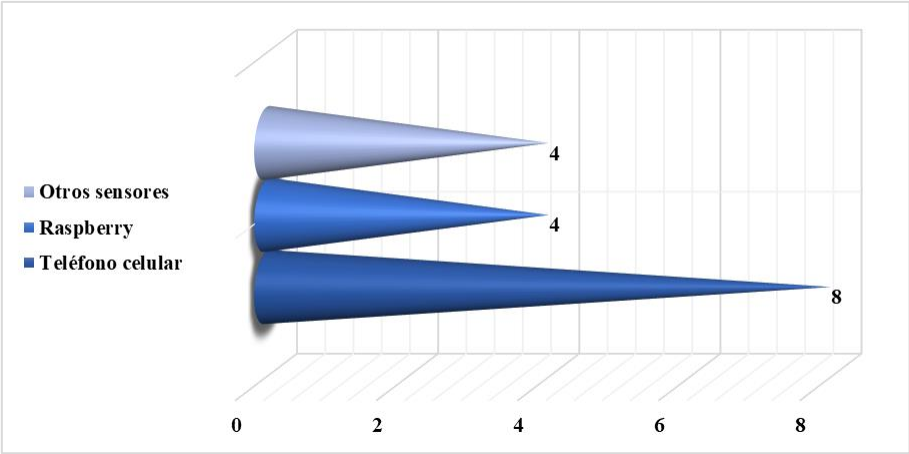


Figura 10. Trabajos que utilizan sensores en dispositivos móviles

Además de utilizar BkC e IoT, algunos artículos utilizaron otras tecnologías adicionales: unos artículos utilizan Edge network y Fog computing para acelerar el traspaso y procesamiento de datos, otros utilizan Inteligencia Artificial para predicción de enfermedades o síntomas, y otros utilizan Swarm nodes para asegurar la transferencia descentralizada entre nodos (ver Fig. 11).

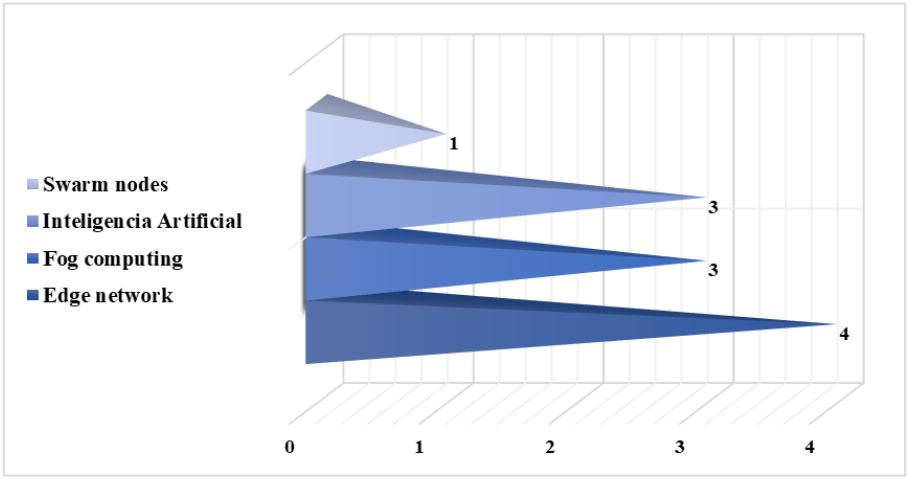


Figura 11. Trabajos que utilizan varias tecnologías

El 96% de los artículos sí presentaron Diagramas para representar la propuesta en BkC e IoT, otro 56% utilizaron Sensores médicos IoT, otro 56% utilizaron Servicios en nube, otro 37% si nombraron Aplicaciones informáticas, además el 56% si realizaron Pruebas o Simulaciones,

por otra parte el 48% si nombraron o especificaron el software que utilizaron para implementar la propuesta, y sólo en el 19% se enfocaron en seguimiento de COVID-19. En el 56% de las propuestas aplicaron las características nombradas para lograr sus propios objetivos.

Entre los 7 factores de cada artículo (Diagrama, Sensores médicos IoT, Servicios en nube, Aplicaciones informáticas, Pruebas o simulación,Especifica software, Estudia Covid-19), si el articulo utiliza ese factor se le asigna un punto sino es cero; en la Fig. 12 el cuadro verde significa 1 porque si lo utiliza, además se adicionó el país de procedencia, año de producción; la Viabilidad es la suma de los factores entre 1 y 7; se considera que el artículo es Aplicable si la viabilidad es mayor e igual que 4 puntos y se presentan con círculo verde, si la viabilidad es menor e igual que 3 puntos no es viable y se presentan con círculo amarillo; es decir si es 57% de su puntaje el artículo es aplicable.

Son viables el 52% de los artículos, en otras palabras 14 de los 27 artículos son aplicables a hospitales para el contexto ecuatoriano.

Figura 12. Factores viables

4. DISCUSIÓN

El seguimiento y control de pacientes es importante con la ayuda de dispositivos IoT en forma regular, rápida y automática, además estos datos de salud deben ser compartidos a doctores y otros interesados en forma segura y privada mediante BkC, por esta razón se propone un modelo basado en estas dos tecnologías. Se definió un modelo de conexión y datos para el seguimiento de pacientes de hospitales basado en las investigaciones y los componentes son adoptados de estas investigaciones para tener un fundamento científico. La comunicación es directa entre pacientes y doctores a través de los dispositivos IoT, los demás participantes no interfieren o no obstruyen el seguimiento del paciente a través de alertas emitidas desde la red blockchain.

Existen varios desafíos en la combinación de BkC e IoT en el área de salud como: escalabilidad, procesamiento, el almacenamiento que está en continuo aumento, aumentar las habilidades de las personas en estas tecnologías, legalizar el uso de BkC en el área de salud, desarrollos en otras áreas [50], (Yogeshwar & Kamalakkannan, 2021).

Se realiza una revisión de la literatura en bibliotecas virtuales, y se obtuvo 27 artículos científicos relevantes para el modelo propuesto, se tabulan los datos en una hoja electrónica, se clasifica, categoriza y determina la viabilidad de los artículos en el contexto ecuatoriano.

Existe lugar para potenciar el modelo propuesto en la integración de dispositivos IoT más livianos o ligeros o protocolos más seguros en estos dispositivos, además otra posible mejora es la adición de incentivos para que los pacientes obtengan descuento al comprar de medicinas en farmacias privadas, por otra parte la acumulación de estos datos puede servir para pronósticos de enfermedades o análisis mediante Inteligencia Artificial.

5. CONCLUSIÓN

Mediante una revisión de literatura de los últimos tres años se identificaron 27 diferentes modelos que realizan procesos de conexión y envío de datos que utilizan las tecnologías BkC e IoT en salud, con objetivos concretos como el *Monitoreo en Salud, Alerta de salud, Interoperabilidad y Seguimiento de diabetes*. La *seguridad, privacidad, recolección y comunicación de datos* son las funciones más utilizadas por las propuestas BkC e IoT en salud.

Basados en tecnologías Blockchain e IoT se establece un modelo de conexión y datos para el seguimiento de los pacientes de hospitales, el modelo propuesto está formado por 6 niveles con sus funciones y estructura de datos definidas.

Mediante la contrastación de trabajos previos se evalúa la metodología de estudio y se establece una tabla de factores viables del modelo aplicable a hospitales en el contexto ecuatoriano.

REFERENCIAS

A, H. P., Senthilmurugan, M., K, P. R., & Chinnaiyan, R. (2021). IoT and Machine Learning based Peer to Peer Platform for Crop Growth and Disease Monitoring System using Blockchain. *2021 International Conference on Computer Communication and Informatics (ICCCI)*, 1–5. https://doi.org/10.1109/ICCCI50826.2021.9402435

Abou-Nassar, E. M., Iliyasu, A. M., El-Kafrawy, P. M., Song, O.-Y., Bashir, A. K., & El-Latif, A. A. A. (2020). DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access*, *8*, 111223–111238. https://doi.org/10.1109/ACCESS.2020.2999468

Adamy, A., & Rani, H. A. (2022). An evaluation of community satisfaction with the government's COVID-19 pandemic response in Aceh, Indonesia. *International Journal of Disaster Risk Reduction*, *69*, 102723. https://doi.org/10.1016/J.IJDRR.2021.102723

Aguirre Sánchez, M. J. (2021). *Tecnologías de Seguridad en Bases de Datos: Revisión Sistemática*. http://dspace.ups.edu.ec/handle/123456789/20566

Al-Kumaim, N. H., Alhazmi, A. K., Mohammed, F., Gazem, N. A., Shabbir, M. S., & Fazea, Y. (2021). Exploring the Impact of the COVID-19 Pandemic on University Students' Learning Life: An Integrated Conceptual Motivational Model for Sustainable and Healthy Online Learning. *Sustainability 2021, Vol. 13, Page 2546*, *13*(5), 2546. https://doi.org/10.3390/SU13052546

Alam, S. R., Jain, S., & Doriya, R. (2021). Security threats and solutions to IoT using Blockchain: A Review. *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, *Iciccs*, 268–273. https://doi.org/10.1109/ICICCS51141.2021.9432325

Alamri, B., Javed, I. T., & Margaria, T. (2021). A GDPR-Compliant Framework for IoT-Based Personal Health Records Using Blockchain. *2021 11th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2021*. https://doi.org/10.1109/NTMS49979.2021.9432661

AlJemy, K., AlAnazi, M., AlSofiry, M., & Baig, A. (2019). Improving IoT Security Using Blockchain. *2019 IEEE 10th GCC Conference & Exhibition (GCC)*, 1–6. https://doi.org/10.1109/GCC45510.2019.1570521015

Apuzzo, M., & Kirkpatrick, D. D. (2020). Covid-19 changed how the world does science, together. *New York Times*, *1*.

Aujla, G. S., & Jindal, A. (2021). A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring. *IEEE Journal on Selected Areas in Communications*, *39*(2), 491–499. https://doi.org/10.1109/JSAC.2020.3020655

Azbeg, K., Ouchetto, O., Andaloussi, S. J., Fetjah, L., & Sekkaki, A. (2018). Blockchain and IoT for Security and Privacy: A Platform for Diabetes Self-management. *2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech)*, 1–5. https://doi.org/10.1109/CloudTech.2018.8713343

Bhattacharya, P., Mehta, P., Tanwar, S., Obaidat, M. S., & Hsiao, K.-F. (2020). HeaL: A blockchain-envisioned signcryption scheme for healthcare IoT ecosystems. *2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, 1–6. https://doi.org/10.1109/CCCI49893.2020.9256705

Celiz, R. C., De La Cruz, Y. E., & Sanchez, D. M. (2019). Cloud Model for Purchase Management in Health Sector of Peru based on IoT and Blockchain. *2019 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2018*, 328–334. https://doi.org/10.1109/IEMCON.2018.8615063

Chévez Morán, M. J. (2021). *Estudio de los patrones de seguridad para la atenuación de las irregularidades, las debilidades y amenazas en empresas de servicios de telecomunicaciones*. http://dspace.ups.edu.ec/handle/123456789/20568

Devibala, A. (2019). A Survey on Security Issues in Iot for Blockchain Healthcare. *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 1–7. https://doi.org/10.1109/ICECCT.2019.8869253

Dwivedi, A. D., Malina, L., Dzurenda, P., & Srivastava, G. (2019). Optimized Blockchain Model for

Internet of Things based Healthcare Applications. *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, 135–139. https://doi.org/10.1109/TSP.2019.8769060

Fernández-Caramés, T. M., Froiz-Míguez, I., Blanco-Novoa, O., & Fraga-Lamas, P. (2019). Enabling the Internet of Mobile Crowdsourcing Health Things: A Mobile Fog Computing, Blockchain and IoT Based Continuous Glucose Monitoring System for Diabetes Mellitus Research and Care. *Sensors*, *19*(15), 3319. https://doi.org/10.3390/s19153319

Firouzi, F., & Farahani, B. (2021). Harnessing the Power of Smart and Connected Health to Tackle COVID-19: IoT, AI, Robotics, and Blockchain for a Better World. *IEEE Internet of Things Journal*, *8*(16), 12826–12846. https://doi.org/10.1109/JIOT.2021.3073904

Garg, L., Chukwu, E., Nasser, N., Chakraborty, C., & Garg, G. (2020). Anonymity Preserving IoT-Based COVID-19 and Other Infectious Disease Contact Tracing Model. *IEEE Access*, *8*, 159402–159414. https://doi.org/10.1109/ACCESS.2020.3020513

Guaigua Bucheli, C. J. (2021). *Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistemático*. https://dspace.ups.edu.ec/handle/123456789/20319

Guaman Villalta, M. G. (2021). *Hyperledger Blockchain para la seguridad en bases de datos un mapeo sistemático*. https://dspace.ups.edu.ec/handle/123456789/20320

Hewa, T., Braeken, A., Ylianttila, M., & Liyanage, M. (2020). Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT. *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, *2020-Janua*, 1–6. https://doi.org/10.1109/GLOBECOM42002.2020.9348125

Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020*, 310–317. https://doi.org/10.1109/ICIoT48696.2020.9089570

Juyal, S., Sharma, S., Harbola, A., & Shukla, A. S. (2020). Privacy and Security of IoT based Skin Monitoring System using Blockchain Approach. *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 1–5. https://doi.org/10.1109/CONECCT50063.2020.9198409

Karthikeyyan, P., Velliangiri, S., & Joseph. S, M. I. T. (2019). Review of Blockchain based IoT application and its security issues. *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, 6–11. https://doi.org/10.1109/ICICICT46008.2019.8993124

Kaschel, H., & Diaz, A. (2021). High Security Ubiquitous H-IoT on a WBAN-based EHR using Blockchain. *2021 IEEE International Conference on Automation/XXIV Congress of the Chilean Association of Automatic Control (ICA-ACCA)*, 1–6. https://doi.org/10.1109/ICAACCA51523.2021.9465266

Khalil, H., Tamara, L., Rada, G., & Akl, E. A. (2022). Challenges of evidence synthesis during the 2020 COVID pandemic: a scoping review. *Journal of Clinical Epidemiology*, *142*, 10–18. https://doi.org/10.1016/J.JCLINEPI.2021.10.017

Llerena Izquierdo, J., Naranjo Sánchez, R., Zambrano Santos, M., & Espol. (2018). *Sistema de información geográfico socioeconómico y del medio ambiente*. https://www.dspace.espol.edu.ec/handle/123456789/43942

Llerena Izquierdo, J., Ortiz Rojas, J. G., Mora Saltos, N. S., & Freire, L. (2009, February 20). *Sistema de Gestión de Asistencia Institucional, SIGAI*. https://www.dspace.espol.edu.ec/handle/123456789/767

Majeed, A. (2021). Effective Handling of COVID-19 Pandemic: Experiences and Lessons from the Perspective of South Korea. *COVID 2021, Vol. 1, Pages 325-334*, *1*(1), 325–334. https://doi.org/10.3390/COVID1010026

Mallikarjuna, B., Kiranmayee, D., Saritha, V., & Krishna, P. V. (2021). Development of Efficient E-Health Records Using IoT and Blockchain Technology. *ICC 2021 - IEEE International Conference on Communications*, 1–7. https://doi.org/10.1109/ICC42927.2021.9500390

McBroome, J., Martin, J., Schneider, A. de B., Turakhia, Y., & Corbett-Detig, R. (2022). Identifying

SARS-CoV-2 regional introductions and transmission clusters in real time. *MedRxiv*, 2022.01.07.22268918. https://doi.org/10.1101/2022.01.07.22268918

Melendrez-Caicedo, G., & Llerena-Izquierdo, J. (2022). Secure Data Model for the Healthcare Industry in Ecuador Using Blockchain Technology. *Smart Innovation, Systems and Technologies*, *252*, 479–489. https://doi.org/10.1007/978-981-16-4126-8_43

Miranda Jiménez, J. N. (2021). *Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos*. http://dspace.ups.edu.ec/handle/123456789/20966

Morán Maldonado, N. M. (2021). *Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática*. http://dspace.ups.edu.ec/handle/123456789/20243

Muñoz Campuzano, P. S. (2021). *Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20932

Pérez-Ch, S., Pinto, R., & Sánchez, R. (2021). Blockchain as a tool in patient monitoring affected by Covid-19. *REVISTA PUCE*, 17–42.

Ponce Larreategui, J. G. (2021). *Indicadores de compromiso (IOC) para detección de amenazas en la seguridad informática con enfoque en el código malicioso*. http://dspace.ups.edu.ec/handle/123456789/20937

Primahendra, R., Sumbogo, T. A., Lensun, R. A., & Purwanto, A. (2020). Handling Corona Virus Pandemic In The Indonesian Political Context: A Grounded Theory Study. *European Journal of Molecular & Clinical Medicine*, *7*(8), 113–129. https://ejmcm.com/article_3000.html

Rahman, M. A., Shamim Hossain, M., Islam, M. S., Alrajeh, N. A., & Muhammad, G. (2020). Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. *IEEE Access*, *8*, 205071–205087. https://doi.org/10.1109/ACCESS.2020.3037474

Rakib, G. A., Saiful Islam, M., Rahman, M. A., Maruf Syed, A., Hossain, M. S., Alrajeh, N. A., & Saddik, A. El. (2021). DeepHealth: A Secure Framework to Manage Health Certificates Through Medical IoT, Blockchain and Deep Learning. *2021 IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, 1–6. https://doi.org/10.1109/MeMeA52024.2021.9478691

Ramane, R., Patole, R., Nevrekar, S., Aher, A., & Deshmukh, N. (2021). Monitoring Health of IIOT Devices using Blockchain. *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, 300–304. https://doi.org/10.1109/ICIEM51511.2021.9445282

Ray, P. P., Chowhan, B., Kumar, N., & Almogren, A. (2021). BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem. *IEEE Internet of Things Journal*, *8*(13), 10857–10872. https://doi.org/10.1109/JIOT.2021.3050703

Ray, P. P., Dash, Di., Salah, K., & Kumar, N. (2021). Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. *IEEE Systems Journal*, *15*(1), 85–94. https://doi.org/10.1109/JSYST.2020.2963840

Saha, S., Sutrala, A. K., Das, A. K., Kumar, N., & Rodrigues, J. J. P. C. (2020). On the Design of Blockchain-Based Access Control Protocol for IoT-Enabled Healthcare Applications. *IEEE International Conference on Communications*, *2020-June*, 0–5. https://doi.org/10.1109/ICC40277.2020.9148915

Salazar, L. (2018). *Implementación de sistema de matriculación y carnetización en la unidad educativa Pablo Picasso.* http://dspace.ups.edu.ec/handle/123456789/16844

Sánchez Guzmán, C. O. (2021). *Modelo de red segura en un entorno distribuido para la transferencia de datos con mecanismos básicos de seguridad*. https://dspace.ups.edu.ec/handle/123456789/20321

Srivastava, G., Crichigno, J., & Dhar, S. (2019). A Light and Secure Healthcare Blockchain for IoT Medical Devices. *2019 IEEE Canadian Conference of Electrical and Computer Engineering, CCECE 2019*. https://doi.org/10.1109/CCECE.2019.8861593

Tahir, M., Sardaraz, M., Muhammad, S., & Saud Khan, M. (2020). A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics. *Sustainability*, *12*(17), 6960. https://doi.org/10.3390/su12176960

Terán Terranova, Y. J. (2021). *Seguridad en la Gestión de la información para las organizaciones públicas desde el enfoque ISO/IEC 2700: un Mapeo Sistemático*. https://dspace.ups.edu.ec/handle/123456789/20333

Wolkewitz, M., & Puljak, L. (2020). Methodological challenges of analysing COVID-19 data during the pandemic. *BMC Medical Research Methodology*, *20*(1), 1–4. https://doi.org/10.1186/S12874-020-00972-6/METRICS

Xiang, X., Wang, M., & Fan, W. (2020). A permissioned blockchain-based identity management and user authentication scheme for e-health systems. *IEEE Access*, *8*, 171771–171783. https://doi.org/10.1109/ACCESS.2020.3022429

Yogeshwar, A., & Kamalakkannan, S. (2021). Healthcare Domain in IoT with Blockchain Based Security- A Researcher's Perspectives. *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, *Iciccs*, 1–9. https://doi.org/10.1109/ICICCS51141.2021.9432198

Zhang, Q., Gao, J., Wu, J. T., Cao, Z., & Zeng, D. D. (2022). Data science approaches to confronting the COVID-19 pandemic: a narrative review. *Philosophical Transactions of the Royal Society A*, *380*(2214). https://doi.org/10.1098/RSTA.2021.0127