UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

EVALUACIÓN DE ARQUITECTURA BLOCKCHAIN MA-ABS PARA LA GESTIÓN DE HISTORIAS CLÍNICAS ELECTRÓNICAS PERUANAS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor:

Bach. Martínez Montenegro Fernando Daniel

ORCID: https://orcid.org/0000-0002-8698-7859

Asesor:

Mg. Tuesta Monteza Victor Alexci

ORCID: https://orcid.org/0000-0002-5913-990X

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú

2022

Aprobación del jurado

EVALUACIÓN DE ARQUITECTURA BLOCKCHAIN MA-ABS PARA LA GESTIÓN DE HISTORIAS CLÍNICAS ELECTRÓNICAS PERUANAS

Bach. Martínez Montenegro Fernando Daniel
Autor

Mg. Tuesta Monteza Victor Alexci
Asesor

Mg. Bravo Ruiz Jaime Arturo
Presidente

Mg. Tuesta Monteza Victor Alexci
Secretario

MBA. Bances Saavedra David Enrique
Vocal

Dedicatoria

Dedico este trabajo principalmente a Dios y a mis padres, por haberme dado la vida y permitirme haber llegado hasta este momento tan importante de mi formación profesional. A mis hermanos que siempre me han brindado su apoyo incondicional y son las personas más importantes en mi vida. A cada docente, amigos y compañeros de clases, con lo que he compartido conocimientos, y momentos gratos en mi carrera Universitaria.

El Autor

Agradecimientos

Agradezco en primer lugar a Dios por permitirme lograr mis metas y objetivos, y darme las fuerzas para elaborar este informe de investigación, a mis padres por ser el pilar de mi vida, a mi asesor y a mis docentes universitarios, que me guiaron en el transcurso de mi vida universitaria.

El Autor

Resumen

Las historias clínicas actualmente están cambiando en los establecimientos médicos, de la forma tradicional de llevar en manera manuscrita, a utilizar sistemas informáticos para llevarlos de manera electrónica. Las historias clínicas electrónicas, permiten ser actualizadas por más de una persona a la vez desde diferentes ubicaciones, facilitando el intercambio de información y comunicación entre los médicos. Esto está ocasionando varios desafíos como la centralización de los datos de los pacientes y la privacidad del manejo de información, y de cumplir normas de protección de datos, seguridad de información y la transmisión de dichos documentos a distintos proveedores de salud. Una de las tecnologías que está solucionando estos problemas es Blockchain; esta tecnología está ganando popularidad con un entorno distribuido y descentralizado, y sin la necesidad de contar con un intermediario. En esta investigación luego de realizar una búsqueda en las diferentes bases de datos de artículos científicos según ranking de Scimago, se modelará la arquitectura Blockchain MA-ABS, según sus características y su esquema, así como la creación de la cadena de bloque, mediante el servicio que brinda la plataforma tecnológica IBM Blockchain e Hyperledger Fabric, y se centrará en realizar pruebas a los indicadores de privacidad y seguridad con la ayuda del desarrollo de una aplicación de gestión de historias clínicas. Esta tecnología Blockchain permite la seguridad de los datos y la privacidad de la información y logrará realizar un consenso entre las entidades distribuidas sin depender de una sola. Por lo que se concluye que la arquitectura Blockchain planteada nos brinda mayor seguridad en el control de acceso, obteniendo un cien por ciento en las tareas realizadas del control de acceso y privacidad en la información de las historias clínicas de los pacientes, teniendo como resultado cero filtraciones de la información del paciente. Además, se recomienda evaluar otras métricas de los indicadores de privacidad de información y seguridad de datos de la arquitectura Blockchain para la obtención de resultados similares.

Palabras Clave

Blockchain, Arquitectura Blockchain, Historia clínica electrónica, Hyperledger Fabric, privacidad, seguridad, cuidado de la salud.

Abstrac

Medical records are currently changing in medical establishments from the traditional handwritten form of record keeping to the use of computerised systems for electronic record keeping. Electronic medical records allow them to be updated by more than one person at a time from different locations, facilitating the exchange of information and communication between doctors. This is causing several challenges such as centralisation of patient data and privacy of information handling, and complying with data protection standards, information security and the transmission of such documents to different healthcare providers. One of the technologies that is solving these problems is Blockchain; this technology is gaining popularity with a distributed and decentralised environment, and without the need for an intermediary. In this research after conducting a search in the different databases of scientific articles according to Scimago ranking, the Blockchain MA-ABS architecture will be modelled, according to its characteristics and its scheme, as well as the creation of the blockchain, using the service provided by the IBM Blockchain and Hyperledger Fabric technology platform, and will focus on testing the privacy and security indicators with the help of the development of a medical records management application. This Blockchain technology enables data security and information privacy and will achieve consensus among distributed entities without relying on one single entity. Therefore, it is concluded that the proposed Blockchain architecture provides greater security in access control, obtaining one hundred percent in the tasks performed in access control and privacy in the information of patients' medical records, resulting in zero leaks of patient information. In addition, it is recommended to evaluate other metrics of information privacy and data security indicators of the Blockchain architecture to obtain similar results.

Keywoord

Blockchain, Blockchain architecture, Electronic Health Record, Privacy, Security, Hyperledger Fabric, Healthcare.

Tabla de contenido

Índice de Tablas

Índice de Figuras

I. INTRODUCCIÓN

1.1. Realidad Problemática

En el Perú un gran porcentaje de Instituciones Prestadoras de Servicios de Salud - IPRESS que forman parte de la Superintendencia Nacional de Salud – SUSALUD tiene inconvenientes en la administración de las historias clínicas de los usuarios, como duplicación, perdida o con el hecho de no contar en el instante con los antecedentes de los pacientes(Alarcon-loayza et al., 2019). Por ejemplo, un paciente puede tener uno o más historias clínicas como visitas a centros de salud y en el mismo centro de salud puede tener más de uno(Resolución_Ministerial_N__618-2019-MINSA, 2019), por lo cual una publicación del día 23 del mes de mayo del año 2013, se crea RENHICE mediante la ley 30024(Resolución_Ministerial_N__618-2019-MINSA, 2019), donde permitirá que el usuario puede tener acceso a la información contenida en su HCE, y a los médicos que deberán ser autorizados previamente(Congreso de la República del Perú, 2013b).

Las historias clínicas electrónicas (HCE) miden información personal crucial pero sensible para la designación y el tratamiento de la atención, que requieren ser distribuidos y compartidos a menudo entre pares como establecimientos de salud, compañías de seguros, farmacias, investigadores, familias de pacientes, entre otros(Dubovitskaya et al., 2017). La HCE puede ser actualizada por más de una persona a la vez desde diferentes ubicaciones, facilitando el intercambio de información y comunicación entre los médicos, permite reutilizar y agregar información para generar informes y toma de decisiones a nivel médico y gerencial(Olavarría, 2019). En argentina, los médicos que han pasado de un sistema a otro coinciden en señalar que el proceso de registro de datos de los pacientes en papel demanda mucho más tiempo y espacio físico, en comparación al proceso de registro de datos electrónicos, que simplifica la mayoría de los procesos, agiliza los trámites administrativos, optimiza los recursos y, por ende, permite una mejor atención(Diario Norte, 2019).

Compartir la información sobre la atención puede ayudarnos a ser más inteligentes, por ejemplo, a una mejor comprensión de los patrones de tendencias de salud y enfermedades para confirmar una atención de mayor calidad(Jothi et al., 2015). Por lo tanto, la gestión de HCE impone un desafío para la protección de la privacidad, al tiempo que garantiza la accesibilidad de la información para los pares aprobados y el paciente está destinado a regular la entrega de sus datos únicamente a los pares en los que confía, y este debe ser accesible para numerosos pares de establecimientos completamente diferentes(de Oliveira et al., 2019). El tener acceso a las acciones que realizan los participantes de la red como por ejemplo las modificaciones de los permisos de los pacientes, la actualización o el intercambio de información realizada por un médico, estás deben ser restringidas debido a los riesgos de seguridad de los datos o la filtración de información privada del paciente, así mismo las HCE actuales son administradas por hospitales y proveedores, mientras que los pacientes se ven privados del derecho de controlar libremente sus propias HCE(Guo et al., 2018); por lo cual existe una preocupación en los médicos el papel del ordenador ya que es influyente en los aspectos de los sistemas de las HCE, debido a la calidad de información y la seguridad contenida en ellos(De Medicina et al., 2016).

En el año 2015, por los motivos de escasez de protección de datos electrónicos y de recursos empleados para la garantía de la seguridad, se registraron extravíos de datos e información de salud de los pacientes y estas violaciones de privacidad se debieron al robo de los ordenadores portátiles de los médicos y establecimientos médicos (Gestion Medica, 2015). Y este año se han cometido más infracciones en registros de atención médica que en todo 2016, 2017 y 2018 combinados, según se muestra en la Figura 1.

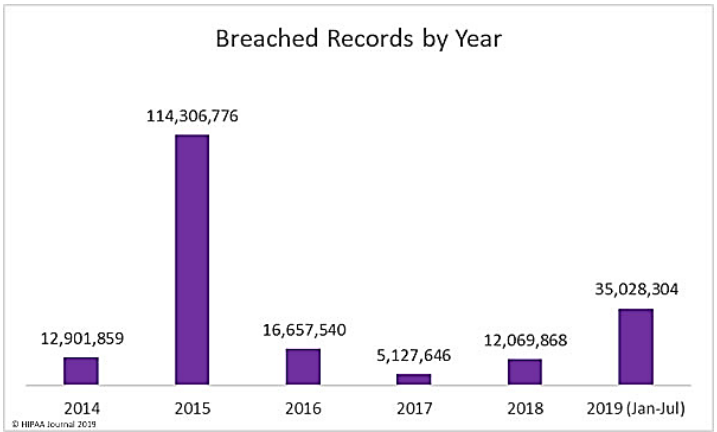


Figura 1. Infracciones de registros médicos por año. Fuente: (HIPAA JOURNAL, 2019)

En la india se utilizó la HCE en la nube por que ayuda a evitar preocuparse por el mantenimiento a servidores físicos y por la seguridad(Deshmukh, 2017), en Taiwán para garantizar el acceso a la información y poder controlar la autorización de los pacientes se utilizó las tarjetas con Circuito Integrado(Y.-C. J. Li et al., 2015), asimismo, la tecnología Blockchain permite enviar información de un punto a otro utilizando un nodo de envío seguro y confiable. Si un nodo se vuelve peligroso, se detectará el error y la transmisión se cancelará por completo(Hontoria, 2018).

Existen diferentes proyectos de arquitecturas blockchain, entre ellas tenemos: MedRec(Azaria et al., 2016) es el primer proyecto que implementó arquitectura blockchain, tiene encriptación y seguimiento de auditoria, pero necesita que sus datos sean minados y tiene falta en escalabilidad(Shuaib et al., 2019), Medicalchain(Abdullah, 2018) permite la comunicación entre diferentes médicos, tiene una mayor seguridad y privacidad gracias hacia su doble encriptación y está centrado en el paciente, pero no tiene control sobre sus token y requiere de la criptomoneda(Shuaib et al., 2019), MediBChain(Omar et al., 2019) es un proyecto de arquitectura blockchain en el cual solo los nodos registrado pueden participar y no se puede acceder a la información sin ser procesados por los otros nodos; pero no existe interoperabilidad y los contratos inteligentes necesitan de criptomoneda(Shuaib et al., 2019), Modum.io AG(Bocek et al., 2017).

Al proporcionar la herramienta para lograr el consenso entre las entidades distribuidas sin depender de una sola parte confiable, la tecnología blockchain permite la seguridad de los datos, el control sobre los datos confidenciales y facilitará la gestión de datos de atención médica para el paciente y los diferentes actores en el ámbito médico(Dubovitskaya et al., 2017). Blockchain se encuentra entre las siete principales tendencias tecnológicas emergentes de Gartner, las cuales impactarán y transformarán las industrias hasta el 2030(Panetta, 2018).

Los dispositivos inteligentes se caracterizarán por los servicios digitales que ofrecerán, ya que serán más sutiles en toda partes(Cearley, 2018). En la Figura 2 muestra que la tecnología blockchain relacionada a la salud es una de las tendencias de las industrias tecnológicas emergentes.

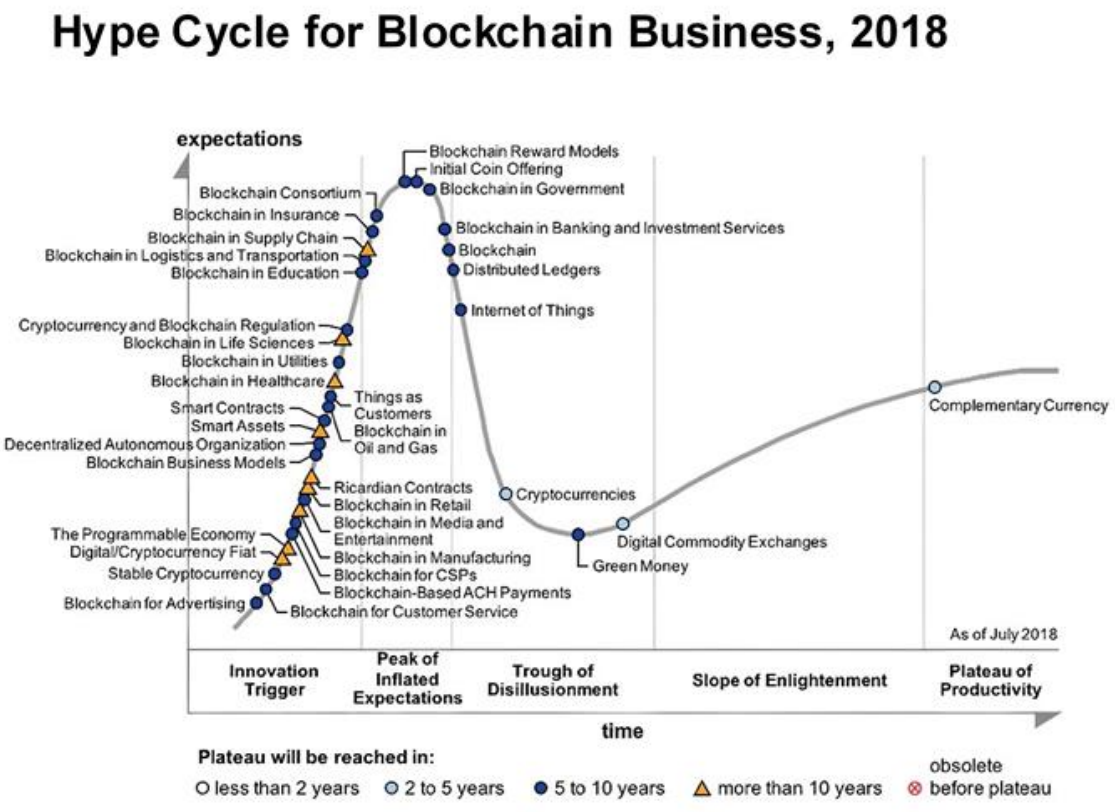


Figura 2. Hype Cycle for Blockchain Business, 2018 Fuente: (Levy, 2018)

En esta investigación se propone la evaluación de la arquitectura blockchain utilizando el esquema de firmado basado en atributos en múltiples

autoridades (MA-ABS) en la gestión de historias clínicas electrónicas peruanas. Esta arquitectura aborda tres principales problemas destacados anteriormente: la interoperabilidad del sistema, la privacidad de la información y la seguridad de los datos de los pacientes.

1.2. Trabajos Previos.

G. Yang and C. Li, (2018) realizó la investigación, “A design of blockchain-based architecture for the security of electronic health record (EHR) systems”, en Noruega. Una solución de Blockchain para mejorar la interoperabilidad de los sistemas EHR actuales, evitar la manipulación y el uso malicioso de los EHR. Además, incluir un nuevo mecanismo de incentivos para la creación de nuevos bloques en la cadena de bloques. Los accesos a los registros de estado en estas bases de datos del servidor SQL deben pasar por la cadena de bloques, que luego realiza un seguimiento de todos los registros de consultas, como seleccionar, insertar y eliminar, etc., asimismo solo permiten que los proveedores participen en el mantenimiento de la cadena de bloques. La asignación de derechos de acceso a un registro debe ser aprobada por el usuario en el contrato resumido. Y concluyen que la arquitectura es independiente de cualquier plataforma específica de blockchain y está abierta a más extensiones, y solo permiten que los proveedores asuman las principales responsabilidades de mantenimiento de la cadena de bloques, incluida la creación, verificación y anexión de nuevos bloques.

M. T. de Oliveira et al, (2019) realizó la investigación “Towards a Blockchain-based Secure Electronic Medical Record for Healthcare Applications”, en China. Un enfoque basado en blockchain para asegurar EMR para aplicaciones de atención médica, donde el control de acceso se centra en el paciente. También, mantiene los EMR cifrados en la cadena de bloques, y el paciente comparte la clave de descifrado solo con los médicos en los que confía. Los resultados muestran que se escala bien ya que aumentar el número de nodos en la red implica un aumento lineal en el tamaño de la cadena almacenada. Los resultados también revelan que el tiempo para

insertar un nuevo EMR en la cadena de bloques sigue siendo bajo, incluso cuando aumenta el número de nodos en la red.

F. Tang, S. Ma, Y. Xiang, and C. Lin, (2019) realizó la investigación “An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records”, en China. En la creación de un nuevo paradigma de EHR que puede ayudar a lidiar con el problema centralizado de los EHR basados en la nube. Nuestra solución es utilizar la tecnología emergente de blockchain para EHR (denominada EHR basada en blockchain para mayor comodidad). En primer lugar, definimos formalmente el modelo de sistema de EHR basados en blockchain en la configuración de consorcio blockchain. Además, el problema de autenticación es muy importante para los EHR. Nuestra propuesta es un esquema de firma basado en la identidad con múltiples autoridades que pueden resistir el ataque de colusión de N de N - 1 autoridades. Además, nuestro esquema es demostrablemente seguro en el modelo de oráculo aleatorio y tiene algoritmos de firma y verificación más eficientes que los esquemas de autenticación existentes de EHR basados en blockchain.

A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, (2016) realizó la investigación “MedRec: Using Blockchain for Medical Data Access and Permission Management”, en Austria. MedRec: un nuevo sistema de gestión de casos descentralizado para el procesamiento de EMR utilizando tecnología blockchain. Este sistema proporciona a los pacientes registros completos e inmutables y proporciona un fácil acceso a su información de salud en todos los médicos y entornos de tratamiento. MedRec gestiona la autenticación, la seguridad, la responsabilidad y el intercambio de datos aprovechando las propiedades únicas de la cadena de bloques. Esta es una consideración importante al procesar información confidencial. Las soluciones de almacenamiento de datos locales se integra al diseño modular existente del proveedor para promover la interoperabilidad y hacer que el sistema sea asequible y adaptable. Alentamos a los profesionales de la salud (investigadores, autoridades de salud pública, etc.) a unirse a la red como "menores" de blockchain. Esto les proporciona acceso a datos

agregados y anónimos como recompensas de minería, a cambio de mantener y asegurar la red a través de Prueba de trabajo. Por lo tanto, big data proporciona empoderar a los investigadores y es esto permite el surgimiento de una economía de datos y, al mismo tiempo, atraer la opción de exponer metadatos a pacientes y proveedores.

S. Rahmadika and K. H. Rhee, (2018) realizó la investigación “Blockchain technology for providing an architecture model of decentralized personal health information”, en Republica de Korea. Un modelo conceptual para administrar los datos de PHI que se derivan de varios proveedores de atención médica al confiar en la tecnología blockchain en la red de superposición punto a punto. Además, elaboramos el análisis de seguridad que podría estar ocurriendo en el modelo propuesto. Al aprovechar nuestro modelo, permite a los pacientes y a los proveedores recopilar de manera efectiva los datos de PHI en una sola vista, así como garantizar la integridad de los datos. El blockchain ofrece un registro inmutable del dato sin tener que confiar en un tercero. Los resultados muestran que el enfoque propuesto promete desarrollarse debido a la alta tasa de éxito en términos de difusión de datos.

R. Guo, H. Shi, Q. Zhao, and D. Zheng, (2018) realizó la investigación “Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems”, en China. La validez de los EHR encapsulados en blockchain, presentamos un esquema de firma basado en atributos con múltiples autoridades, en el que un paciente respalda un mensaje de acuerdo con el atributo sin revelar ninguna otra información que no sea la evidencia de que ha atestiguado eso. Además, existen múltiples autoridades sin una única central o de confianza para generar y distribuir claves públicas / privadas del paciente, lo que evita el problema de custodia y se ajusta al modo de almacenamiento de datos distribuidos en la cadena de bloques. Al compartir las semillas secretas de la función pseudoaleatoria secreta entre las autoridades, este protocolo resiste el ataque de colusión de N de las autoridades corruptas N-1. Bajo el supuesto de Diffie-Hellman bilineal computacional, también demostramos

formalmente que, en términos de la imperdonabilidad y la privacidad perfecta del firmante de atributos, este esquema de firma basado en atributos es seguro en el modelo de oráculo aleatorio. La comparación muestra la eficiencia y las propiedades entre el método propuesto y los métodos propuestos en otros estudios.

Omar, Bhuiyan, Basu, Kiyomoto, & Rahman, (2019) realizó la investigación "Privacy-friendly Platform for Healthcare Data in Cloud Based on Blockchain Environment", en EE.UU. Un sistema de gestión de datos de atención médica centrado en el paciente que utiliza la tecnología blockchain como almacenamiento que ayuda a lograr la privacidad. Utilizando las funciones criptográficas para encriptar los datos de los pacientes y garantizar el seudónimo, y analizamos los procedimientos de procesamiento de datos y también la rentabilidad de los contratos inteligentes utilizados en nuestro sistema. Por lo cual, nuestra plataforma garantiza que los datos de atención médica privada en la nube sean controlados solo por los propios pacientes y logramos seudonimato mediante el uso de funciones criptográficas. Y concluimos que nuestra plataforma cumple con los requisitos de seguridad y privacidad para los sistemas de administración de datos de atención médica y la evaluación experimental del rendimiento muestra que esta plataforma funciona bien en un entorno blockchain.

Attia, Khoufi, Laouiti, & Adjih, (2019) realizó la investigación "An IoT-Blockchain Architecture Based on Hyperledger Framework For Healthcare Monitoring Application", en España. Una arquitectura de seguridad basada en el marco Fabric Hyperledger. Validamos nuestro enfoque primero a nivel de diseño a través de ejemplos concretos, luego mostrando algunas funcionalidades implementadas. Asimismo, diseñamos e implementamos una arquitectura IoT segura para el dominio de la aplicación de atención médica, basada en la tecnología blockchain. el trabajo se centrará en configurar una red blockchain utilizando el marco Fabric proporcionado por Hyperledger y diseñar una interfaz gráfica de usuario (GUI) que permita a un usuario dentro de la red mostrar su libro mayor en visualizaciones y paneles claros. Y concluyen que los datos muestran las últimas horas y

permite al trabajador de la salud establecer una comparación entre los resultados y el estado del paciente.

Radhakrishnan, Sam Joseph, & Sudhakar, (2019) realizó la investigación "Securing Blockchain based Electronic Health Record using Multilevel Authentication", en India. Un esquema basado en autenticación multinivel para proteger la cadena de bloques de los ataques de phishing, billeteras frías basadas en diccionarios y calientes. El sistema propuesto se divide en cuatro capas, como la Capa de gestión de usuarios, la Capa de generación y visualización de EHR, la Capa de almacenamiento de EHR y la Capa de gestión de acceso de EHR según la funcionalidad. Como resultado tenemos que el acceso a la aplicación de atención médica necesita el número móvil registrado, la contraseña y la contraseña de un solo uso generadas por el autenticador y el privilegio de acceso del usuario se decide en función de su rol. Y concluyen que la aplicación de atención médica basada en blockchain tiene una capa adicional de seguridad que utiliza una contraseña de un solo uso que elimina los ataques basados en la billetera del usuario.

Cao, Zhao, Wang, Su, & Ji, (2011) realizó la investigación "Multi-authority attribute-based signature", en Japón. Un esquema ABS de múltiples autoridades, que respalde políticas complejas, expresando AND, OR y condiciones de umbral. Utilizando una autoridad central para asegurar la usabilidad de las claves de atributos que un usuario obtiene de diferentes autoridades de atributos. Este esquema respalda cualquier política expresiva y construye la seguridad bajo la suposición estándar de Diffie-Hellman simultáneamente, lo que no solo cumple con el requisito de aplicaciones reales, sino que también reduce la confianza de una autoridad, al tiempo que mantiene las propiedades de ABS, la imperdibilidad y la privacidad del firmante de atributos. Y concluyen que su esquema puede ajustarse a los requisitos de las aplicaciones reales y también distribuir la confianza a todas las autoridades del sistema.

1.3. Teorías relacionadas al tema.

1.3.1. Historia clínica

La historia clínica (HC) es un documento de derecho médico que captura secuencialmente datos de atención al paciente, conocimientos y procesos relacionados y los integra con la atención brindada por profesionales de la salud de manera ordenada e inmediata. Debe adjuntar una firma digital o manuscrita. Estos registros médicos son administradas por las IPRESS(MINSA, 2018).

1.3.1.1. Archivo de las historias clínicas

Según la Resolución Ministerial 214-2018/MINSA (2018), se debe tener en cuenta lo siguiente, para el archivo de las historias clínicas:

1) Según su relevancia legal, histórica o científica, se determina su ubicación en:
   a) Archivo Común de Historias Clínicas

      Se clasifican las historias clínicas según su frecuencia de uso(MINSA, 2018).

   b) Archivo Especial de Historias Clínicas

      Aquí se pueden encontrar las historias clínicas según interés legal, o pacientes que tengan cáncer ocupacional, estos documentos tienen un alto nivel de seguridad.(MINSA, 2018).

2) La Frecuencia de Uso, se tiene en cuentan los siguientes aspectos:
   a) Archivo Activo

      Son los archivos que son constantemente solicitados por el personal médico, durante los últimos cinco años (MINSA, 2018).

   b) Archivo Pasivo

Son los archivos que por más de cinco años no han concurrido a la IPRESS, y estos serán conservados por quince años en dependencias nacionales o regionales (MINSA, 2018).

Las historias deben pasar del archivo pasivo al archivo activo, si por alguna razón el personal de salud hace uso nuevamente de los servicios, conservando la misma identificación(MINSA, 2018).

3) Aquellas IPRESS que cuenten con un SIHC, deben plasmar aspectos de disponibilidad, integridad, confidencialidad, autenticidad y seguridad, conforme a ley(MINJUS, 2013) y con la firma de los médicos(MINSA, 2016) al registrar la acción y use la firma del médico y las actividades de salud. Y firmas digitales para usuarios saludables (incluidas firmas electrónicas). Pueden emitirse imprimiendo formularios de atención y manteniendo registros médicos escritos a mano. Además, deben tenerse en cuenta los siguientes puntos:

   a) Debe realizarse por el profesional médico y estar alojado en el sistema informático(MINSA, 2018).

   b) La IPRESS debe asegurar que la trazabilidad de los datos se realicen por única vez, autentificándose mediante credenciales de acceso (MINSA, 2018).

   c) El consentimiento informado debe seguir la normatividad, para la firma electrónica del paciente (MINSA, 2018).

   d) Los tutores firmaran electrónicamente en casos de menores de edad para los formatos de atención(MINSA, 2018).

4) Para retirar una historia clínica se debe regir según normatividad.

1.3.1.2. Estructura de la historia clínica

1) Identificación del paciente, contiene los datos que identifican al paciente, como puede ser su DNI, pasaporte o carnet de extranjería, según corresponda, así como los datos de la IPRESS (Congreso de la República del Perú, 2011).

2) Registro de la atención

   En este documento se encuentra la atención que se brindará al usuario de salud o paciente(MINSA, 2018).

3) Información complementaria

   Además de la información anterior se debe considerar registros de sustento administrativo, técnico, legal y/o científico, así como exámenes auxiliares elaboradas al momento de la atención del paciente. También el formato de registros de seguros, referencia y Contrarreferencia y del consentimiento informado si fuese pertinente(Congreso de la República del Perú, 2011).

1.3.1.3. Formatos de la historia clínica

Según la Resolución Ministerial 214-2018/MINSA (2018), el contenido mínimo de variables que deben estar incluidas en cada formato se específica a continuación:

1) Formatos Básicos.

Formatos en Consulta Externa en el Primer Nivel de Atención

(1) Formato de Atención Integral de la Niña y el Niño

(2) Formato de Atención Integral del Adolescente

(3) Formato de Atención Integral del Joven

(4) Formato de Atención Integral del Adulto

(5) Formato de Atención Integral del Adulto Mayor

En Hospitales e Institutos Especializados.

Formatos en Emergencia.

Formatos en Hospitalización.

Ficha Familiar

Figura 3. Formatos Básicos de Historias Clínicas. Fuente: (MINSA, 2018)

2) Formatos Especiales

Representan a los documentos restantes no consignados dentro de los formatos básicos, entre estos formatos tenemos:

Tabla 1

Formatos Especiales de Historias Clínicas

Formatos Especiales de Historias Clínicas	
Formato de Filiación.	
Notas de Enfermería.	
Hoja de Control de Medicamentos u Hoja de Control Visible.	
Gráfica de Signos Vitales	
Hojas de Balance Hidro-Electrolítico.	
Formato de Interconsulta	
(1) Solicitud de Interconsulta	(2) Informe de Interconsulta
Orden de Intervención Quirúrgica.	
Reporte Operatorio	
Formatos de Anestesia.	
(1) Hoja de Evaluación Pre Anestésica.	(2) Hoja de Anestesia.
(3) Hoja Post Anestésica.	
Formato de la Historia Clínica Materno Perinatal	
Notas de Obstetricia.	
Fichas Odonto-Estomatolóficas.	
(1) Ficha del Niño	(2) Ficha del Adolescente, Joven, Adulto y Adulto Mayor.
(3) Ficha de la Gestante	
Formatos de Patología Clínica.	
Formatos de Diagnóstico por Imágenes.	
Formatos de Anatomía Patológica.	
Formato de Consentimiento Informado.	
Formato de Retiro Voluntario.	
Formato de Referencia y Contrarreferencia.	
Informe de Alta.	

Fuente: (MINSA, 2018)

1.3.2. Historia clínica electrónica

Se trata de un registro médico que contiene un archivo multimedia personal unificado en una base de datos electrónica, registrado mediante un programa informático y firmado electrónicamente por el personal médico. La actualización, almacenamiento y uso se realizan bajo estrictas condiciones de seguridad, precisión, integridad, confiabilidad, inteligibilidad, confidencialidad, almacenamiento, acceso y uso de usabilidad, tales como 'aprobados por Minsa(Congreso de la República del Perú, 2013b).

Además de lo dispuesto en la Ley N° 30024, y su Reglamento, debe tenerse en cuenta lo siguiente:

a) El historial médico se escribe o se envía de forma electrónica para cada persona tratada en un centro médico. Esto debe hacerse gradualmente en medios electrónicos accesibles a los médicos aprobados por IPRESS bajo el marco regulatorio aplicable.(MINSA, 2018).

b) Las IPRESS podrán optar por el uso de la HCE, debiendo sujetarse a las mismas disposiciones establecidas de las HC en papel, tanto en aspectos clínicos como legales, además el acceso y registro de información de la salud de los pacientes(MINSA, 2011).

c) Los servicios de apoyo privados, públicos o mixtos brindan apoyo regular al mismo paciente y, según lo exige la ley, reconocen el sistema de información si están sujetos a la inscripción continua del tratamiento brindado(Congreso de la República del Perú, 2013b).

d) Las HCE igual que las HC en papel deberán estar refrendadas por una firma, la cual sería una firma digital la cual tendrá la misma eficacia y validez jurídica, según lo señalado en la Ley(Congreso de la República del Perú, 2000).

e) La estructura de la HCE, debe separar los datos de identificación del paciente como sus atenciones, y se podrán combinar únicamente en la atención de prestación asistencial del paciente(MINSA, 2018).

f) El sistema de información de HCE debe revisarse periódicamente dentro de las autoridades sanitarias. Cada comité de agencia de registro sanitario verifica el cumplimiento del control de calidad en el registro. El comité de auditoría de salud o el comité de revisión de salud establecido por IPRESS realiza evaluaciones a través de estos grupos, y si estos grupos no están disponibles, el comité organizador de historia clínica los revisará(MINSA, 2018).

g) Deberán adaptarse e implementar al sistema de HCE progresivamente, aquellas IPRESS públicas, privadas o mixtas que aun cuenten con Historias Clínicas en papel, según su disponibilidad presupuestal, y deberán cumplir con los estándares para la acreditación de su sistema ante RENHICE(MINSA, 2018).

h) La implementación de registros de salud electrónicos en IPRESS no significa que los registros de salud escritos a mano existentes que se encuentran en ellos deban convertirse a una versión electrónica (MINSA, 2018).

i) Deberán implementar aquellas IPRESS públicas, privadas o mixtas que tengan su sistema informatizado de Historias Clínicas a un sistema de información de HCE para ser acreditados por RENHICE(MINSA, 2018).

j) La HCE debe ser auditable, permitir la secuencia de las atenciones y la impresión.

Tabla 2

Diferencias entre la historia clínica en papel e historia clínica electrónica

VARIABLE	HISTORIA CLINICA PAPEL	HISTORIA CLINICA ELECTRÓNICA
Almacenamiento	Mayor almacenamiento y alto costo	Almacenamiento virtual reducido y costo económico.
Calidad de la información	Puede haber duplicidad de información y de tratamientos.	Evita redundancia de tratamientos.
Continuidad de los actos registrados	Se puede modificar la continuidad temporal de los sucesos.	Son registrados cronológicamente los actos y hechos.
Disponibilidad	Solo se encuentra disponible para una persona y está en un solo lugar.	Se encuentra disponible de manera simultánea, en cualquier lugar y en cualquier momento.
Durabilidad	Los documentos sufren deterioro por degradación, por su uso o por otros factores por el transcurso del tiempo.	La información permanece en el tiempo inalterable para ser consultada.
Fecha y Hora	La fecha y hora no siempre es registrada.	La fecha y hora se registra siempre.
Identificación del que consulta la información	No existe un control de usuarios que acceden a la información.	Existe un control de identificación de los usuarios que accedan a la información.
Información	El ingreso de información es parcial, debido a la omisión de algunos campos.	El ingreso de información es completo debido a los campos obligatorios.
Ingreso de datos	Se registra según el estilo del personal.	Cumple un estándar.
Médico tratante	No siempre aparece el nombre y la firma del médico.	El médico siempre se identifica.
Redacción	La redacción de la información no siempre es legible.	La redacción de la información es legible.

Reserva de la información	Los mecanismos que garantizan la reserva de información no siempre son eficientes.	Cumple con mecanismos que garantizan la reserva de información.
Seguridad de la información	Es alto el riesgo de pérdida de la información.	El riesgo de pérdida de información es mínimo debido a los backs up realizados.
Transferencia de la información	La transferencia se realiza de manera física.	La transferencia se realiza de manera virtual y siempre están a disposición del paciente.

Fuente: (Congreso de la República del Perú, 2013a)

1.3.3. Fundamentos de la tecnología blockchain.

Los inicios de blockchain se remontan a un documento escrito por (Nakamoto, 2008). Él introdujo una versión peer-to-peer de dinero electrónico, bitcoin, que permite que los pagos en línea se envíen directamente entre las partes sin pasar por intermediarios financieros centralizados. Como parte de la implementación de bitcoin, Nakamoto también ideó el libro de contabilidad, que Nakamoto denominó "una cadena de bloques" (Nakamoto, 2008). Esta cadena de bloques es compatible con la nueva versión del efectivo electrónico (The Economist, 2015) y posteriormente se denominó cadena de bloques. Muchas otras tecnologías de blockchain se han desarrollado desde que Nakamoto introdujo por primera vez el blockchain.

Blockchain proporciona una base de datos digital descentralizada de transacciones, también conocida como libro mayor distribuido, que se mantiene y actualiza mediante una red de computadoras que verifican una transacción antes de que se apruebe y agregue al libro mayor. Permite a las partes que realizan transacciones intercambiar la propiedad de los activos representados digitalmente en un sistema de igual a igual en tiempo real e inmutable sin el uso de intermediarios(Morkunas et al., 2019). La Figura 3 ilustra los seis

pasos del intercambio de activos entre dos actores económicos que utilizan la tecnología blockchain.

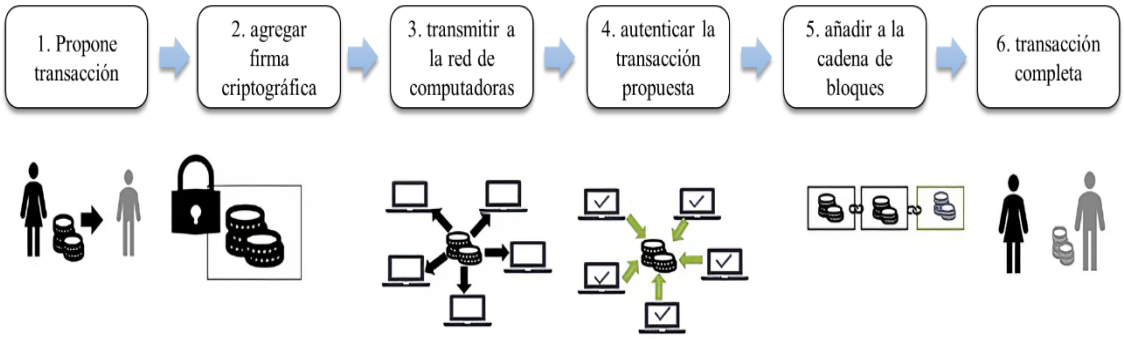


Figura 4. Los seis pasos del intercambio de activos usando blockchain
Fuente: (Morkunas et al., 2019)

1.3.4. Blockchain

No hay una estructura centralizada o jerárquica en la red de blockchain. Un blockchain es un sistema descentralizado que consta de seis capas: datos, red, consenso, contrato, servicio y aplicación. La recopilación de datos, la validación y la manipulación se procesan principalmente dentro de las capas de datos y de red (Alphand et al., 2018). Las capas de consenso y contrato incluyen contratos inteligentes, protocolos de consenso y mecanismos de incentivos (Eyal & Sirer, 2018). Las capas de servicio y aplicación implementan en la práctica actividades basadas en blockchain (Marc, 2016). En la Tabla 1, se enumera brevemente los componentes o tecnologías asociadas con las seis capas, respectivamente. Como protocolo de promoción, un mecanismo de incentivo podría construirse como una capa separada (Nakamoto, 2008). La capa de incentivo se utiliza principalmente para varias criptomonedas; su objetivo es promover el intercambio de recursos, estimular la inteligencia grupal y promover la comunicación colaborativa. En la práctica industrial, las plataformas de consorcios y blockchain privadas se establecen para un grupo específico, en lugar de para todos. Por lo tanto, los mecanismos de

incentivo o las actividades mineras no son obligatorias. Este cambio es más propicio para las comunicaciones y transacciones entre los participantes en los sistemas de cadena de bloques más amplios (Xie et al., 2018). De acuerdo con la arquitectura, el blockchain incluye tres elementos centrales: una estructura de bloque de cadena basada en la marca de tiempo, un mecanismo de almacenamiento distribuido basado en una red P2P y un mecanismo de consenso basado en nodos descentralizados (Yuan & Wang, 2018).

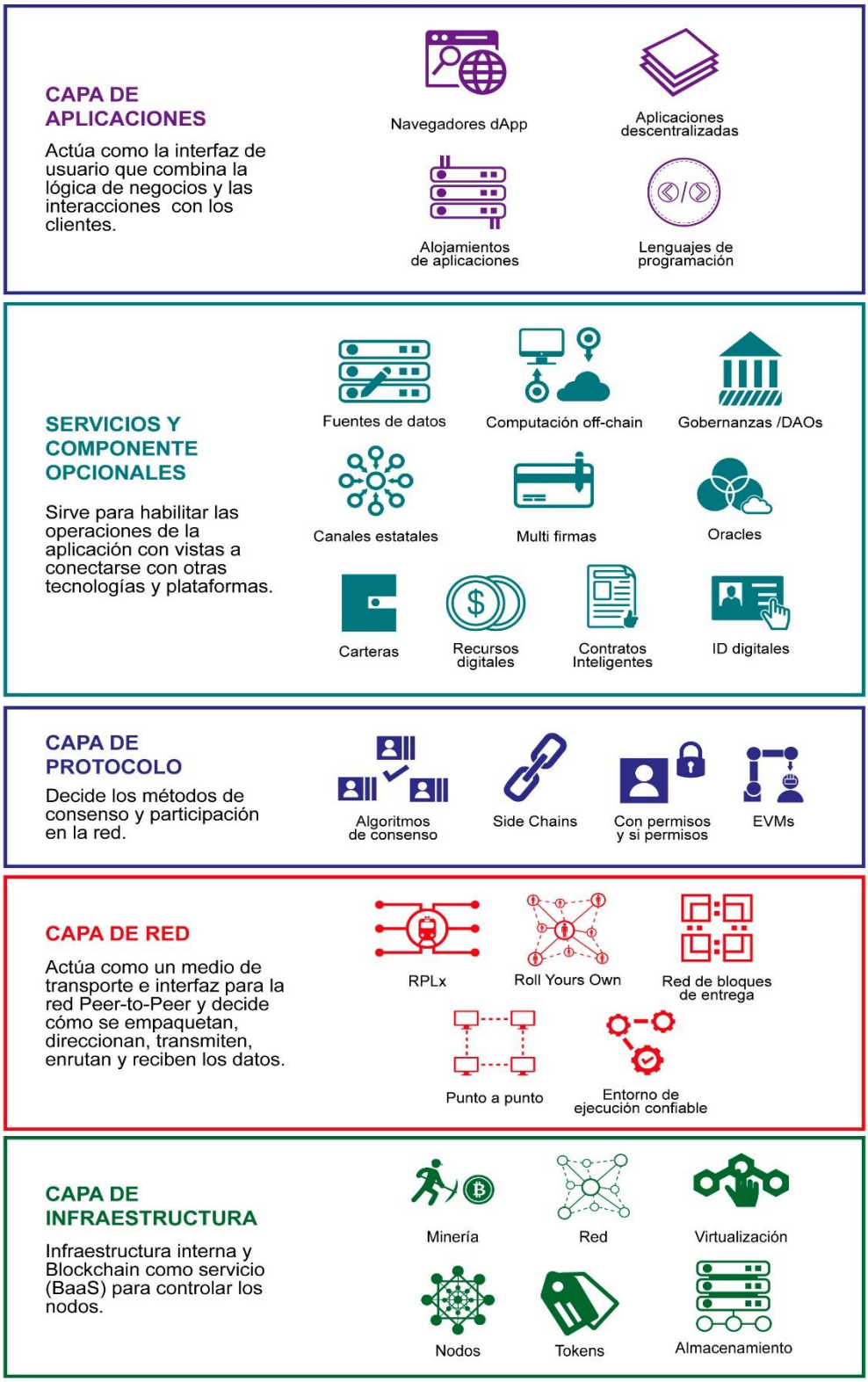


Figura 5. Componentes del Blockchain Fuente: (Rodriguez, 2018)

1.3.5. La estructura de blockchains

Blockchain se componen de tres partes principales:

1) Bloque: una lista de transacciones registradas en un libro mayor durante un período determinado. El tamaño, el período y el evento desencadenante de los bloques es diferente para cada cadena de bloques.

   No todas las blockchains están grabando y asegurando un registro del movimiento de su criptomoneda como su objetivo principal. Pero todas las cadenas de bloques registran el movimiento de su criptomoneda o token. Piense en la transacción como simplemente el registro de datos. Asignarle un valor (como sucede en una transacción financiera) se utiliza para interpretar qué significan esos datos(Laurence, 2017).

2) Cadena: Un hash que une un bloque a otro, matemáticamente "encadenándolos" juntos. Este es uno de los conceptos más difíciles de comprender en blockchain. También es la magia que une las cadenas de bloques y les permite crear confianza matemática.

   El hash en blockchain se crea a partir de los datos que estaban en el bloque anterior. El hash es una huella digital de estos datos y bloquea los bloques en orden y tiempo.

   Aunque las blockchains son una innovación relativamente nueva, el hashing no lo es. El hash fue inventado hace más de 30 años. Esta vieja innovación se está utilizando porque crea una función unidireccional que no se puede descifrar. Una función de hash crea un algoritmo matemático que asigna datos de cualquier tamaño a una cadena de bits de un tamaño fijo. Una cadena de bits suele tener una longitud de 32 caracteres, que luego representa los datos que se han procesado. El algoritmo de hash seguro (SHA) es una de algunas funciones de hash criptográficas utilizadas en

blockchains. SHA-256 es un algoritmo común que genera un hash de 256 bits (32 bytes) de tamaño fijo casi único. Para fines prácticos, piense en un hash como una huella digital de datos que se usa para bloquearlo en su lugar dentro de la cadena de bloques(Laurence, 2017).

3) Red: La red está compuesta de "nodos completos". Piense en ellos como la computadora que ejecuta un algoritmo que protege la red. Cada nodo contiene un registro completo de todas las transacciones que alguna vez se registraron en esa cadena de bloques.

   Los nodos se encuentran en todo el mundo y pueden ser operados por cualquier persona. Operar un nodo completo es difícil, costoso y requiere mucho tiempo, por lo que las personas no lo hacen de forma gratuita. Se les incentiva a operar un nodo porque quieren ganar criptomonedas. El algoritmo blockchain subyacente los recompensa por su servicio. La recompensa generalmente es un token o criptomoneda, como Bitcoin(Laurence, 2017).

1.3.6. Tipos de blockchain

Blockchains públicos a los que todos pueden acceder y actualizar, tiene blockchains privados para que solo un grupo limitado dentro de una organización pueda acceder y actualizar, y tiene un tercer tipo, un consorcio de blockchains que se utilizan en colaboración con otros.

A. Blockchains públicos

En la cadena de bloques pública, en lugar de usar un servidor central, la cadena de bloques está asegurada por verificación criptográfica respaldada por incentivos para los mineros. Cualquiera puede ser un minero para agregar y publicar esas transacciones. En la blockchain pública, está abierta para cualquier persona interesa en verificar las transacciones mediante

el uso de sus recursos de hardware y software y resolviendo un problema de rompecabezas criptográfico(Bambara & Allen, 2018).

B. Blockchains de Consorcio

Un blockchain de consorcio es un libro mayor distribuido donde el proceso de consenso está controlado por un conjunto preseleccionado de nodos. Blockchain puede ser leído de forma restringida o puede ser publica a los participantes, pero también pueden ser hibridas (Bambara & Allen, 2018), es decir ciertos usuarios están autorizados a ingresar transacciones, mientras que otros usuarios tienen derechos de solo lectura(Schneider Zurich, 2017).

C. Blockchains privados

Blockchain privada son cadena de bloques donde los participantes tienen permisos de escritura y se mantienen centralizados en la organización. Los permisos de lectura pueden estar estrictamente por invitación o pueden ser públicos. Las cadenas de bloques privadas podrían proporcionar soluciones a los problemas de las empresas financieras, incluidos los agentes de cumplimiento de las reglamentaciones, como la Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA), las leyes contra el lavado de dinero (AML) y las leyes de conocimiento de sus clientes (KYC)(Bambara & Allen, 2018).

Tabla 3

Diferencias y similitudes entre blockchains.

	Blockchain Publicas	**Blockchain Privadas**	**Blockchain Hibridas**
Se pueden solventarse	NO	SI	SI
Contratos inteligentes	SI	SI	SI
Único administrador	NO	SI	NO
Administrador uno o más	NO	NO	SI
Pueden ser mineros	SI	NO	NO
Recompensas con cryptos	SI	NO	NO
Transparencia	SI	NO	NO

Fuente: (Coral, 2018)

1.3.7. Mecanismos de consenso de blockchain

a) Proof of Work (PoW)

PoW funciona de la siguiente manera: toda la información contenida en un bloque candidato se calcula por su valor hash. Este valor hash generado debe cumplir con los criterios de nivel de dificultad determinados por el sistema. Si el valor hash no cumple con los criterios, el cálculo se repetirá cambiando el valor del sustantivo (número una vez). Nonce es un valor que no tiene ningún significado, pero se agrega intencionalmente al bloque para generar un valor hash de acuerdo con las condiciones. Si el valor hash no cumple con el valor de la regla, el valor nonce cambiará nuevamente hasta que el minero encuentre un valor hash que cumpla con los criterios(Gervais, 2016).

b) Proof of Stake (PoS)

Es la alternativa más común a la Prueba de trabajo. Es una forma alternativa de crear bloques en una cadena de bloques. Los productores de bloques se denominan validadores en lugar de mineros. Los validadores deben depositar un depósito o participación para participar en el proceso de creación de bloques(Dhariwal, 2018).

Aquí, los validadores se seleccionan sobre la base de un algoritmo de selección que tiene en cuenta su participación. Solo el validador seleccionado puede crear un bloque y otros no pueden participar, ahorrando así la energía de los otros validadores. Es mucho mejor para el medio ambiente. Si el validador hace algo incorrecto, pierde su apuesta y, por lo tanto, obtienes una recompensa por tu honestidad. Los mineros toman sus tarifas de transacción porque no obtienen recompensa a diferencia de PoW(Dhariwal, 2018).

c) Proof of Burn

La Prueba de quemadura es una alternativa a la Prueba de trabajo y Prueba de participación y también un método para el consenso distribuido. También es un mecanismo de consenso implementado por una red blockchain para garantizar que todos los nodos participantes lleguen a un acuerdo sobre el estado verdadero y válido de la red blockchain, evitando así cualquier posibilidad de doble gasto en criptomonedas(Dhariwal, 2018).

Funciona según el principio de permitir que los mineros "quemen" o "destruyan" los tokens de moneda virtual, lo que les otorga el derecho de escribir bloques en proporción a las monedas quemadas. Cuantas más monedas quemes, más posibilidades tendrás de ser seleccionado para extraer el siguiente bloque. Intenta abordar el problema del consumo de energía de PoW. Para quemar las monedas, los mineros deben enviarlas a la dirección donde no podrían gastarse para verificar el bloqueo.

Slim coin se basa en este algoritmo de mecanismo de consenso(Dhariwal, 2018).

d) Proof of Capacity (PoC)

Bueno, este también es un algoritmo de mecanismo de consenso. Esto es un poco diferente de otros algoritmos. Aquí pagas por el espacio en disco. Cuanta más capacidad de disco duro tenga, más posibilidades tendrá de eliminar el siguiente bloque y obtener recompensas por bloque. Antes de operar en un sistema PoC, el algoritmo genera un gran conjunto de datos llamado "lote" y los almacena en el disco duro(Dhariwal, 2018).

Esto implica lo siguiente, existe el trazado del disco duro y la eliminación real de los bloques. Dependiendo del tamaño de su disco duro, puede llevar días o incluso semanas crear sus archivos de trama únicos. El trazado utiliza un hash muy lento conocido como Shabal. Esto también incluye variaciones como Prueba de espacio y Prueba de almacenamiento. Esto es más como un juego para pagar. La única criptomoneda que se basa en PoC es la moneda Burst(Dhariwal, 2018).

e) Delegated Proof of Stake (DPoS)

Esta es una extensión de PoS. En el protocolo de consenso de la cadena de bloques DPoS, los titulares de criptomonedas usan el saldo de sus monedas para seleccionar un agente llamado testigo. Estas cookies tienen la capacidad de proporcionar nuevos bloques de transacciones y agregarlos a la cadena de bloques. El poder de voto en realidad está determinado por el número de monedas. Esto se conoce comúnmente como alimentación de red(Dhariwal, 2018).

Si tienes menos monedas no tendrás el mismo impacto de los que tienen más monedas o token. Cualquiera puede participar en la elección del generador de bloques y la posibilidad de crear los

bloques estará determinada por la cantidad de votos que obtengan con respecto a cada otro generador. En el caso de que realmente puedan llevarlo a cabo, en ese momento tendrán que agradecer a los DPoS. La criptomoneda basada en este mecanismo es la moneda CaptainAlt(Dhariwal, 2018).

f) Prueba de actividad

Este algoritmo es mucho más parecido a la Prueba de trabajo con la complejidad reducida en gran medida debido a que la solución del problema toma desde fracciones de segundo a varios minutos. La prueba de actividad es una combinación de prueba de participación y prueba de trabajo. Al igual que PoW, los mineros compiten entre sí para resolver acertijos criptográficos. Luego el sistema cambia a PoS. La diferencia es que los bloques que se extraen no contienen transacciones. Son simplemente plantillas con información de encabezado y la dirección de recompensa minera(Dhariwal, 2018).

La corrección de los bloques creados se verifica limitando el tiempo mínimo posible para la creación del bloque. Esto le permite limitar la velocidad máxima de agregar bloques a la cadena y, por lo tanto, evitar la aparición de inundaciones en la red, que también llamamos spam. Las monedas que usan este mecanismo son Decred y Espers(Dhariwal, 2018).

g) Practical Byzantine fault tolerant Mechanism (PBFT)

PBFT es el protocolo de plataforma blockchain autorizado más popular y actualmente lo utiliza Hyperledger Fabric (IBM). Entonces, ¿has oído hablar del problema del general bizantino? ¿No? Permítanme explicar primero ese problema y luego podrán entender mejor PBFT. Imagina un grupo de generales bizantinos y sus ejércitos rodeando un castillo y preparándose para atacar. Para ganar, deben atacar simultáneamente. Pero saben que hay al menos un traidor entre ellos. Entonces, ¿cómo lanzan un

ataque exitoso con al menos un actor desconocido y malo en su grupo? (Dhariwal, 2018)

La analogía es clara: en cualquier entorno informático distribuido existe el riesgo de que los actores corruptos puedan causar estragos. Por lo tanto, su dependencia del consenso de la comunidad hace que las fallas bizantinas sean un problema especialmente espinoso para blockchain. Para superar ese problema se utiliza PBFT. La decisión presentada por todos los generales determinará una decisión en consenso. El mecanismo de consenso PBFT no requiere ninguna energía de hashing para aprobar los intercambios en una cadena de bloques, lo que implica que no se requiere una alta utilización de energía y el peligro de centralización es menor. También produce altas recompensas y también hay una finalidad de transacción(Dhariwal, 2018).

h) Proof of Elapsed Time

Prueba del tiempo transcurrido es el protocolo de consenso creado por Intel. PoET es ahora el modelo de consenso elegido para el marco modular de Hyperledger Sawtooth. El algoritmo PoET a menudo se usa para otorgar permisos para determinar los derechos que tiene un minero. Las redes que usan esto identifican a los participantes antes de que puedan participar. Cada nodo tiene exactamente la misma posibilidad de ser el ganador del bloque. El mecanismo PoET se basa en difundir y distribuir equitativamente las probabilidades para el mayor número posible de participantes(Dhariwal, 2018).

Cada nodo participante en la red debe esperar una cierta cantidad de tiempo. En esto, cada miembro solicita un tiempo de espera de su enclave local confiable. El miembro con el tiempo de espera más breve es el siguiente en ofrecer un bloqueo después de esperar el tiempo de espera asignado. Cada nodo genera su

propio tiempo de espera cada vez, después de lo cual pasa a una especie de modo de suspensión. Tan pronto como el nodo se despierte y haya un bloque disponible, ese nodo es el afortunado ganador. Luego, un nodo puede difundir la información por toda la red, manteniéndola descentralizada y recibiendo la recompensa(Dhariwal, 2018).

i) Proof of Importance (PoI)

PoI fue introducido por primera vez por NEM para su criptomoneda denominada moneda XEM. Con PoI, no es solo el saldo de la moneda lo que valora. El sistema de recompensas, según el enfoque de PDI, debe basarse en la contribución de un usuario a la red en todas las capacidades. El replanteo del bloque, por lo tanto, se basa en múltiples factores, incluida la reputación, el saldo general y el número de transacciones realizadas a través de o desde una dirección en particular(Dhariwal, 2018).

Aquí, para tener mayor probabilidad de encontrar bloques, son los usuarios que frecuentemente envían y reciben transacciones. La prueba de importancia solo cuenta las monedas que han estado en la cuenta durante varios días. El 10% del XEM que no se ha apartado para la red se repara todos los días. Atacar la red es muy costoso y también recompensa generosamente al usuario por proteger la red(Dhariwal, 2018).

1.3.8. Contrato inteligente en blockchain.

Un contrato inteligente es un lenguaje de programación que se implementa a través de la tecnología de la información. El contrato inteligente apareció mucho antes que la tecnología blockchain. El concepto de contrato inteligente es propuesto por Nick Szabo. Un contrato inteligente es una serie de compromisos definidos en forma digital. Los contratos inteligentes contienen condiciones de ejecución y lógica de ejecución. La lógica de ejecución se ejecuta

automáticamente cuando se cumple la condición. Desde el punto de vista del usuario, un contrato inteligente es un plan de garantía automático. Los contratos inteligentes liberan o transmiten los datos apropiados solo cuando se cumplen ciertas condiciones (Christidis & Member, 2016). Desde una perspectiva técnica, un contrato inteligente es un servidor web. Este servidor no está construido en Internet, pero está construido en blockchains. Por lo tanto, los programas de contrato específicos pueden ejecutarse en estos servidores(Anjana, Kumari, Peri, Rathor, & Somani, 2019). Los contratos inteligentes son la tecnología central de los ledgers compartidos de Blockchain 2.0. Los contratos inteligentes también tienen la capacidad de procesar datos, operar transacciones de activos y administrar activos inteligentes (Bär, Scheife, & Huber, 2006). Los contratos inteligentes amplían la capacidad de la cadena de bloques para manipular datos, pero, al mismo tiempo, imponen mayores exigencias a la seguridad de sus usuarios y sistemas (B, Arnett, Kosba, Miller, & Shi, 2019). Hawk es una arquitectura privada (autorizada) de blockchain que implementa técnicas inteligentes de contrato y compilación para asegurar transacciones en un grupo limitado de participantes que pueden ser seleccionados y verificados (Kosba et al., 2016). Se propuso un protocolo integrado de contrato inteligente para validar la confianza en un ecosistema PKI (infraestructura de clave pública) que será transparente y automático (Lu, 2019)[. Además, algunas investigaciones muestran la capacidad de evaluar la efectividad, la escalabilidad y la viabilidad de los contratos inteligentes. Específicamente, BDD (desarrollo guiado por el comportamiento) y TDD (desarrollo guiado por pruebas) son dos alternativas útiles para verificar y estimar la precisión de los contratos inteligentes (Lu, 2019).

1.3.9. Proyecto de Blockchain

a) Medchain:

La compañía tiene como objetivo utilizar la tecnología blockchain para administrar los registros de salud electrónicos en manos de los pacientes. Esto hace que estas grabaciones sean más seguras y privadas. Actualmente, la compañía ha lanzado una versión beta. También planeamos administrar los datos de los pacientes a través de la aplicación. La red se mantiene mediante una inversión en tokens medchain y se ejecuta en Ether20. Ethereum(Angraal et al., 2017; MedChain, 2019).

Figura 6. Logo de la compañía MedChain Fuente: (MedChain, 2019)

b) Modelchain:

Están trabajando en modelos de atención médica predictiva, haciendo hincapié en que los datos clínicos y los registros médicos se pueden utilizar para predecir la enfermedad de un paciente y recopilar información sobre la vida médica de un paciente. Esto se ve favorecido por la interoperabilidad de las entidades médicas interconectadas. Cambios en los estudios de resultados centrados en el paciente (PCOR) (Liang, Zhao, Shetty, Liu, & Li, 2018).

Figura 7. Logo de la compañía ModelChain Fuente: (Kuo et al., 1385)

c) MA - ABS

En este sistema, hay tres entidades: autoridad de atributo central, autoridades de atributo distribuido y usuarios. La autoridad de atributo central y cada autoridad de atributo tienen sus propias claves privadas para emitir atributos a los usuarios que los solicitan. Además, las autoridades de atributos distribuidos recibirán claves privadas en la configuración de alguna parte confiable, que puede ser la autoridad central. Es posible que estas diferentes autoridades de atributos no confíen entre sí y que ni siquiera se den cuenta. De hecho, algunas de las autoridades de atributos pueden estar corruptas, y esto no debería afectar los atributos adquiridos de otras autoridades. A continuación, damos la definición de ABS con múltiples autoridades de atributos en detalles de la siguiente manera:(J. Li et al., 2010)

Un sistema ABS multi-autoridad se compone de los siguientes cuatro algoritmos:

1) Configuración Este algoritmo lo ejecuta una parte confiable (por ejemplo, la autoridad central). Toma como entrada el parámetro de seguridad λ, este algoritmo genera parámetros de parámetros públicos. Mientras tanto, este algoritmo también devuelve una clave secreta para cada una de las autoridades de atributo, incluida una clave secreta maestra para la autoridad central(J. Li et al., 2010);

2) Extraer Este algoritmo lo ejecuta cada autoridad de atributo. Toma como entrada la clave secreta de la autoridad, la identidad de un usuario u, y un conjunto de atributos en el dominio de esta autoridad. Finalmente, cada autoridad de

atributo devuelve una clave privada de atributo al usuario(J. Li et al., 2010);

3) Firmar Este algoritmo lo ejecuta el usuario. Suponga que un usuario desea firmar un mensaje m con un predicado Y de un conjunto de atributos, toma como entrada su clave privada de atributo para estos atributos y el mensaje emite una firma σ(J. Li et al., 2010).

4) Verificar Al ingresar un mensaje y una supuesta firma, así como las claves públicas de las autoridades de atributos, este algoritmo genera un valor booleano de aceptar o rechazar para indicar si la firma es válida o no(J. Li et al., 2010).

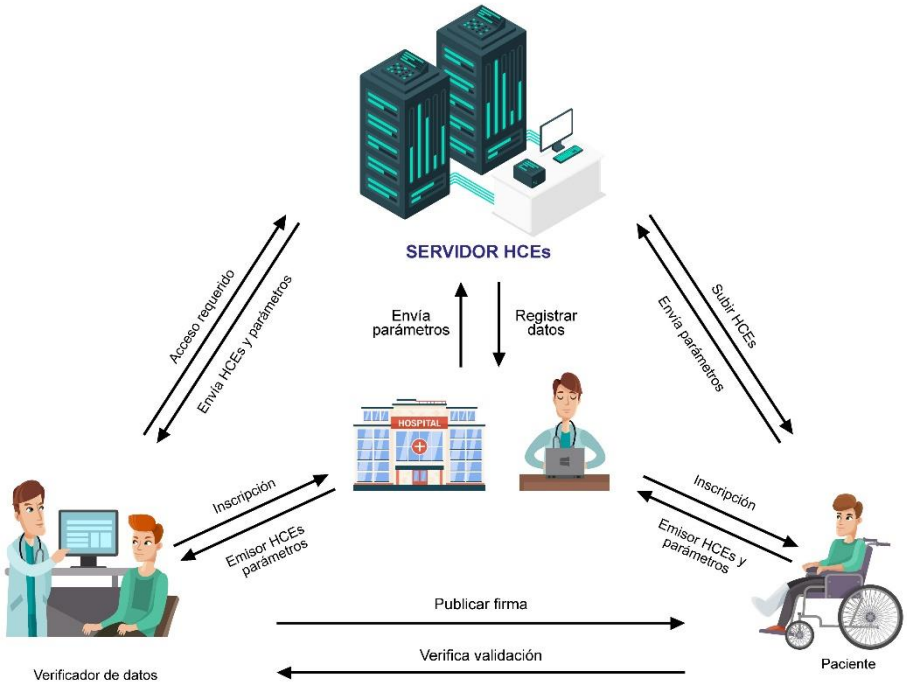


Figura 8. Esquema del sistema MA-ABS Fuente: (Guo et al., 2018)

1.3.10. Proyectos de código abierto basados en blockchain.

a. **Plataforma Ethereum:** En diciembre de 2013, Buterin propuso la plataforma de cadena de bloques Ethereum y un lenguaje de programación completo para redactar contratos inteligentes basados en transacciones de moneda digital Ethernet incorporadas. Ethereum tiene el potencial de crear una computadora mundial descentralizada que nunca se detiene, y que no se censura y se mantiene automáticamente. Ethereum tiene su código abierto en su plataforma de blockchain que utiliza contratos inteligentes para ofrecer servicios o aplicaciones. Ethereum está diseñado para emplear el lenguaje EVM (código de la máquina virtual Ethereum) para ejecutar el programa, y Solidity es el programa de compilación más utilizado (Chen et al., 2016; Wood, 2017).

Figura 9. Logo de la compañía Ethereum Fuente: (Ethereum, 2019)

1) Máquina virtual Ethereum

La máquina virtual Ethereum (EVM) es una potente pila de sandbox virtual integrada en cada nodo de Ethereum completo y responsable de ejecutar el código de bytes del contrato. Los contratos generalmente se escriben en un lenguaje de alto nivel como Solidity y se compilan en código de bytes EVM.

Esto significa que el código de la máquina está completamente aislado de la red, el sistema de archivos o cualquier proceso de la computadora host. Cada nodo en la red Ethereum ejecuta una instancia de EVM que les permite acordar ejecutar las mismas instrucciones. El EVM es Turing completo, que se refiere a un sistema capaz de realizar cualquier paso lógico de una función computacional. JavaScript, el lenguaje de programación que impulsa la web mundial, utiliza ampliamente la integridad de Turing.

Las máquinas virtuales Ethereum se han implementado con éxito en varios lenguajes de programación, incluidos C ++, Java, JavaScript, Python, Ruby y muchos otros.

El EVM es esencial para el Protocolo Ethereum y es instrumental para el motor de consenso del sistema Ethereum. Permite a cualquiera ejecutar código en un

ecosistema sin confianza en el que se puede garantizar el resultado de una ejecución y es totalmente determinista (es decir, ejecutar contratos inteligentes).

b. **Plataforma Hyperledger:** A diferencia de Ethereum y Bitcoin, Hyperledger es un libro de contabilidad distribuido y basado en la empresa, basado en la tecnología blockchain que emplea un contrato inteligente para reforzar la confianza entre los participantes. Hyperledger está diseñado para aplicaciones de cadena de bloques de nivel empresarial e introduce servicios de administración de miembros(Cachin, 2016). En diciembre de 2015, la Fundación Linux lanzó el Proyecto Hyperledger para desarrollar una plataforma de blockchain de negocios de toda la industria. Hyperledger es un blockchain, pero no es una criptomoneda. En el sistema Hyperledger, no es necesario incrustar criptomoneda o actividad minera. El beneficio de este cambio en Hyperledger es el rendimiento de todo el sistema. En general, Hyperledger no aplica hardware específico, software adicional, infraestructura de red o módulos de seguridad. La plataforma Hyperledger es un sistema relativamente adecuado que puede satisfacer los diversos requisitos de las actividades comerciales(Khezr et al., 2019). Hyperledger ofrece múltiples proyectos de blockchain, como Iroha, Cello, Sawtooth, Indy, Explorer, Fabric, Burrow, Caliper, Composer, Quilt, y el proyecto más notable entre ellos es Hyperledger Fabric.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Figura 10. Logo de la compañía Hyperledger Fuente: (Hyperledger, 2019)

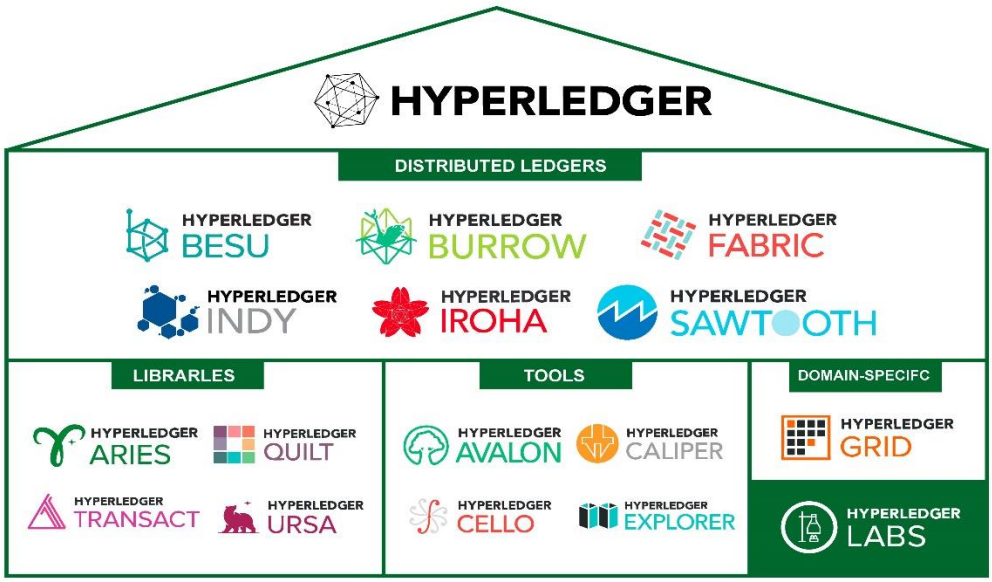


Figura 11. Business Blockchain Frameworks & Tools Hosted by Hyperledger
Fuente: (Hyperledger, 2019)

1) Frameworks

a) Hyperledger Besu: está desarrollado en Java y Apache 2.0. Puede ejecutarse en redes públicas o privadas con licencia Ethereum, así como en redes de prueba como Rinkeby, Ropsten y Görli. Hyperledger Besu incluye varios algoritmos de consenso como PoW, PoA e IBFT y tiene un plan de autorización integral diseñado específicamente para su uso en entornos federados(Hyperledger, 2019).

b) Hyperledger Fabric: Este es el proyecto más famoso de Hyperledger. A diferencia de Ethereum, Fabric es una cadena de bloques delegada y los participantes de la red deben registrarse a través de MSP o un proveedor de servicios para miembros.

Hyperledger Fabric ofrece muchas ventajas. Entre las 6 más importantes están:

1. Compartir solo información necesaria: Hyperledger Fabric permite a las empresas ver solo actividades específicas en grupos específicos (Hurtado, 2018).

2. Autorización: El usuario debe registrarse y soltar el ID. Es importante para las empresas. Porque quiere saber con quién está tratando y, al mismo tiempo, no quiere exponer sus procesos y tecnologías internos a la competencia(Hurtado, 2018).

3. Seguridad: para proteger y administrar las claves, utiliza módulos de seguridad en hardware, esto mejora la protección de los datos confidenciales y la gestión de identificadores (Hurtado, 2018).

4. Modularidad y Plug-In: funciona con el SDK y tiene una estructura modular. Esto permite que se puedan desarrollar redes según las necesidades e ideas de las empresas. Esto hace que el estándar sea muy flexible y relevante para todas las áreas. Los componentes existentes se pueden combinar fácilmente con otras soluciones Blockchain (Hurtado, 2018).

5. Escalabilidad, personalización y confianza: La estructura es modular. Esto mejora la escalabilidad. Puede reducir el nivel de confianza y validación ya que no es necesario incluir todos los operadores de nodo en la transacción. Solo aquellos que están directamente involucrados en una actividad en particular tienen la información(Hurtado, 2018).

c) Hyperledger Indy: Es una plataforma contribuido inicialmente por la Fundación Sovrin, Indy es un proyecto Hyperledger hecho para apoyar la identidad

independiente en libros distribuidos(Gaur et al., 2018). Indy facilita componentes, bibliotecas y herramientas reutilizables las cuales están enraizadas en blockchain donde proporcionan identidades digitales(Gaur et al., 2018).

d) Hyperledger Iroha: Diseñado para proyectos de desarrollo móvil, está basado en Hyperledger Fabric y fue contribuido por Soramitsu, Hitachi, NTT Data y Colu. Presenta un diseño C ++ moderno y controlado por dominio, así como un nuevo algoritmo de consenso tolerante a fallas bizantino basado en cadena llamado Sumeragi(Hyperledger, 2019).

e) Hyperledger Sawtooth: Sawtooth fue aportado por Intel e incluye un novedoso algoritmo de consenso creado por Intel que se llama Prueba de tiempo transcurrido (PoET), que tiene como meta lograr un consenso distribuido de la manera más eficiente posible. Hyperledger Sawtooth tiene potencial en muchas áreas, con soporte para implementaciones autorizadas y sin permiso y reconocimiento de diversos requisitos. Sawtooth está diseñado para brindar versatilidad(Gaur et al., 2018).

2) Herramientas

a) Hyperledger Composer: El Hyperledger Composer (aportado por IBM y Oxchains) construyen redes comerciales blockchain mediante un conjunto de herramientas de colaboración que aumenta el desarrollo de los smart contracts y aplicaciones blockchain, así como su implementación en un libro mayor distribuido(Gaur et al., 2018).

Los componentes principales son:

1. El lenguaje de modelado; lenguaje simple pero expresivo centrado en el negocio (el lenguaje presenta palabras clave como activo y participante) que permite a los no desarrolladores y desarrolladores modelar su red comercial. El lenguaje de modelado también admite el modelado de relaciones y reglas de validación de datos(Hyperledger, 2019).

2. La capacidad de codificar la lógica empresarial como funciones de procesador de transacciones que están escritas en JavaScript estándar. Elegimos JavaScript porque es un lenguaje de programación moderno y de rápida evolución que utilizan millones de desarrolladores de todo el mundo, además de brindarnos la capacidad de ejecutar el código en cualquier lugar que admita JavaScript estándar(Hyperledger, 2019).

3. Control de acceso declarativo mediante listas de control de acceso, que permite a los desarrolladores describir a qué recursos pueden acceder los participantes. El tiempo de ejecución impone automáticamente el control de acceso(Hyperledger, 2019).

4. API de cliente y administrativas, así como una aplicación CLI "compositora" que permite a los desarrolladores y operadores desplegar e interactuar con redes comerciales desde aplicaciones Node.js o scripts de automatización(Hyperledger, 2019).

5. Un "patio de recreo" basado en la web que permite a los usuarios nuevos y experimentados aprender el idioma, modelar su red comercial y probar esa red

desde la comodidad de su navegador web. El patio de recreo puede funcionar tanto en modo "desconectado", utilizando una red simulada como cuando está conectado a una red real(Hyperledger, 2019).

6. Soporte de API REST y capacidades de integración; Se ha desarrollado un conector LoopBack para redes empresariales que expone una red en funcionamiento como una API REST que las aplicaciones cliente pueden consumir fácilmente(Hyperledger, 2019).

7. Soporte de resaltado de sintaxis para dos editores de código abierto populares, Atom y VS Code, con planes futuros sobre cómo podríamos incluir capacidades de prueba / depuración(Hyperledger, 2019).

8. Generación de aplicaciones utilizando el marco Yeoman; los desarrolladores de aplicaciones cliente pueden generar rápidamente una aplicación esqueleto Angular 2 o CLI para usar como punto de partida, lo que les permite enfocarse en UI / UX en lugar de las interacciones de la red empresarial(Hyperledger, 2019).

b) Hyperledger Explorer: puede mostrar, recuperar, distribuir o consultar datos, transacciones o bloques relacionados, información de red, códigos de cadena y familias de transacciones. Es como información mantenida en un registro. Hyperledger Explorer fue ofrecido originalmente por Intel, IBM y DTCC (Hyperledger, 2019).

Hyperledger Explorer se compone de seis componentes clave:

1. Un servidor web: Node.js se utiliza para implementar los componentes del lado del servidor.

2. Una interfaz de usuario web: Angular.js se usa para implementar el marco frontend. Bootstrap se usa por su rica interfaz de usuario y sus características de respuesta(Hyperledger, 2019).

3. WebSockets: las API de WebSocket se utilizan para enviar información del servidor a los clientes.

4. Una base de datos: PostgreSQL es el almacén de datos. La información sobre bloques, transacciones y contratos inteligentes se almacenará en esta base de datos(Hyperledger, 2019).

5. Un repositorio de seguridad: esto actuará como una fachada para implementaciones de seguridad de diferentes plataformas blockchain. Las identidades de usuario y la gestión de acceso se implementarán utilizando un repositorio de seguridad federado(Hyperledger, 2019).

6. Una implementación de blockchain: proporciona actualizaciones sobre transacciones, bloques, registros de nodos y contactos inteligentes al servidor web del explorador(Hyperledger, 2019).

c) Hyperledger Cello: Cello introduce un modelo de entrega "como servicio" bajo demanda en el ecosistema de blockchain, lo que reduce el esfuerzo requerido para crear, administrar y terminar blockchains. Brinde servicios de cadena de múltiples inquilinos de manera eficiente y automática a través de una variedad de infraestructuras, incluidas las máquinas virtuales, las plataformas de

contenedores y múltiples plataformas. Hyperledger Cello fue portado originalmente por IBM y patrocinado por Soramitsu, Huawei e Intel.(Hyperledger, 2019).

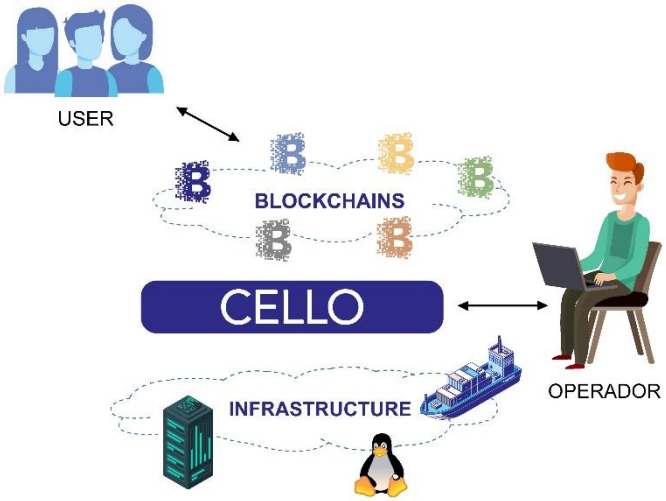


Figura 12. Escenario típico de Hyperledger Cello Fuente: (Hyperledger, 2019)

Basado en tecnologías avanzadas de blockchain y herramientas PaaS modernas, Cello proporciona las siguientes características principales(Hyperledger, 2019):

1. Administre el ciclo de vida de las redes blockchain, por ejemplo, *create/start/stop/delete/keep healthautomáticamente*.

2. Admite configuración de red blockchain personalizada, por ejemplo, tamaño de red, tipo de consenso.

3. Admite múltiples infraestructuras subyacentes, como máquinas virtuales, máquinas virtuales, vSphere, host Docker nativo, enjambre y Kubernetes. Más apoyos en el camino.

4. Se extiende con funciones avanzadas como la capacidad de monitoreo, registro, salud y análisis al integrarse con herramientas existentes como ElasticStack.

d) Hyperledger Quilt: Quilt brinda la interoperabilidad entre los sistemas contables mediante la implementación del protocolo Interledger (también conocido como ILP), que es principalmente un protocolo de pagos y está diseñado para transferir valor entre libros contables distribuidos y libros no distribuidos. El protocolo Interledger proporciona intercambios atómicos entre libros de contabilidad (incluso libros de contabilidad distribuidos o que no son de blockchain) y un espacio de nombre de cuenta único para cuentas dentro de cada libro de contabilidad. Con la incorporación de Quilt a Hyperledger, The Linux Foundation ahora alberga las implementaciones Java (Quilt) y JavaScript (Interledger.js) Interledger(Hyperledger, 2019).

e) Hyperledger Caliper: permite a los usuarios la medición del rendimiento de la implementación de blockchain con un conjunto de casos de uso predefinidos. Hyperledger Caliper producirá informes que contienen una serie de indicadores de rendimiento, como TPS (Transacciones por segundo), latencia de transacción, utilización de recursos, etc. La intención es que los resultados de Caliper sean utilizados por otros proyectos de Hyperledger a medida que desarrollan sus marcos, y como Una referencia para apoyar la elección de una implementación de blockchain adecuada para las necesidades específicas de un usuario. Hyperledger Caliper fue inicialmente contribuido por desarrolladores de Huawei, Hyperchain, Oracle, Bitwise, Soramitsu, IBM y la Universidad de Tecnología y Economía de Budapest(Hyperledger, 2019).

Hyperledger Caliper se puede resumir en dos componentes:

1. Caliper Core: los paquetes Core implementan funciones básicas para la ejecución de un punto de referencia, que incluyen:

    1.1. Caliper CLI: también se proporciona un paquete CLI para la conveniencia de ejecutar un punto de referencia

    1.2. Generación de carga del cliente: los clientes interactúan a través de adaptadores para impulsar una carga de referencia, determinada por un mecanismo de control de velocidad(Hyperledger, 2019).

    1.3. Monitoreo de recursos: contiene operaciones para iniciar / detener un monitor y obtener el estado de consumo de recursos del sistema de cadena de bloques backend, que incluye CPU, memoria, IO de red, etc(Hyperledger, 2019).

    1.4. Análisis de rendimiento: contiene operaciones para leer estadísticas de rendimiento predefinidas (incluyendo TPS, retraso, índice de éxito, etc.) e imprimir resultados de referencia. Las métricas clave se registran al invocar NBIs de blockchain y se usan más tarde para generar las estadísticas(Hyperledger, 2019).

    1.5. Generación de informes: contiene operaciones para generar un informe de prueba en formato HTML

2. Adaptadores Caliper: los adaptadores se utilizan para integrar el sistema blockchain existente en el marco Caliper. Cada adaptador implementa la 'Interfaz de la

cadena de bloques de Caliper' mediante el uso del SDK nativo de la cadena de bloques correspondiente o la API RESTful para mapear operaciones como la implementación de contratos inteligentes en la cadena de bloques del backend, invocar contratos, consultar estados desde el libro mayor, etc(Hyperledger, 2019).

f) Hyperledger URSA: Hyperledger URSA es una biblioteca criptográfica compartida que permitiría evitar la duplicación de herramientas criptográficas, ayudando así a aumentar la seguridad en el proceso. Se trataría de un repositorio disponible para que cualquier proyecto pueda hacer uso de las herramientas criptográficas que necesite. Hyperledger URSA se compone de varios subproyectos, que contienen implementaciones de código o interfaces a código criptográfico. Actualmente hay dos subproyectos (Hyperledger, 2019):

1. La Biblioteca "Base Crypto", cuya principal característica es una biblioteca de firmas modulares compartidas. Esta contiene la implementación de varios esquemas de firmas digitales diferentes con una API común, que permite a los desarrolladores cambiar los esquemas de firmas digitales sobre la marcha (o utilizar y añadir soporte de múltiples esquemas de manera sencilla) (Hyperledger, 2019).

2. Z-mix: El objetivo de este subproyecto es proporcionar una implementación única, flexible y segura para construir pruebas de conocimiento cero (Zeroknowledge proof) (Hyperledger, 2019).

3) Dominio-específico

a) Hyperledger Grid: adopta un enfoque de gestión de la cadena de suministro. La cuadrícula es un ecosistema de tecnologías colaborativas, marcos y bibliotecas que permite a los desarrolladores de aplicaciones elegir los mejores componentes para su industria o modelo de mercado. Hyperledger Grid tiene la intención de proporcionar implementaciones de referencia de tipos de datos centrados en la cadena de suministro, modelos de datos y lógica de negocio basada en contratos inteligentes, todo ello teniendo en cuenta los estándares existentes y las mejores prácticas de la industria. Este framework también servirá para mostrar de manera auténtica y práctica cómo combinar componentes de Hyperledger para desarrollar una solución empresarial única y efectiva(Hyperledger, 2019).

c. Plataforma IBM Blockchain: IBM también lanzó su plataforma Blockchain, que está disponible como parte del catálogo de servicios Bluemix. Está construido sobre el proyecto HyperLedger y ofrece instalaciones adicionales de seguridad e infraestructura para las empresas(Purkayastha, 2019).

Figura 13. Logo de la compañía IBM Blockchain
Fuente: (Purkayastha, 2019)

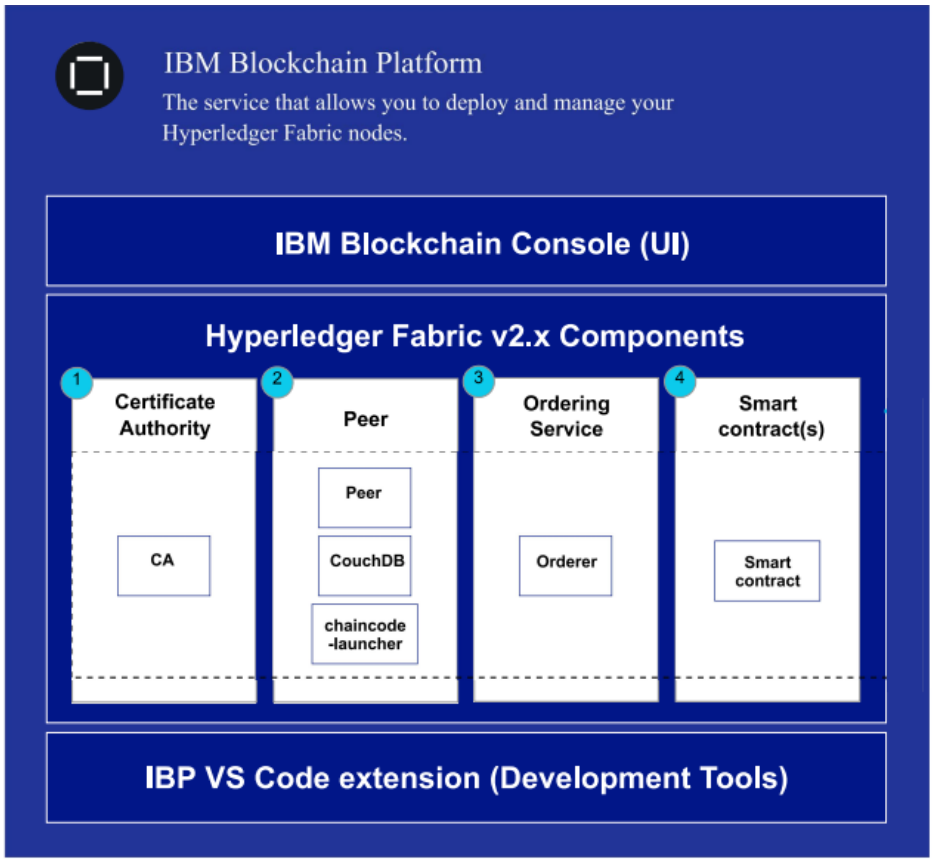


Figura 14. Componentes de la plataforma IBM Blockchain Fuente: (IBM, 2022)

IBM Blockchain Platform Console (UI): Este es el panel de control que le permite crear y administrar sus componentes de la cadena de bloques. Después de proporcionar una instancia de servicio en IBM Cloud, puede implementar la instancia del panel de control de Blockchain de IBM y conéctelo a su clúster en IBM Cloud (IBM, 2022).

Componentes de Hyperledger Fabric: El panel de control se utiliza para crear y administrar componentes de cadenas de bloques según Hyperledger Fabric. Estos componentes se implementan en su clúster y se almacenan a través de la clase de almacenamiento predeterminada cuando se implementa (IBM, 2022).

Extensión de IBM VS Code (herramientas de desarrollo): Descargue la extensión del código VS para comenzar a desarrollar,

empaquetar y revisar las aplicaciones de clientes y los contratos inteligentes (IBM, 2022).

IBM Blockchain Platform, con Hyperledger Fabric se basa en una arquitectura modular y separa en tres fases el procesamiento de transacciones: procesamiento y acuerdo de lógica distribuida ("código de cadena"), ordenación de transacciones y validación y compromiso de transacciones. Esta separación ayuda a algunas ventajas: se necesitan menos niveles de autoconfianza y verificación entre los nodos, las extensiones y la eficiencia de la red optimizada (IBM, 2022).

El ciclo de vida de una transacción en Hyperledger Fabric, comienza con sugerencias de transacción enviadas por una aplicación a un par que la respalda (IBM, 2022). Las estrategias de copia de seguridad describen la cantidad y / o la combinación de copias de seguridad para firmar una propuesta. Luego, los pares que apoyan envían los resultados de la propuesta firmadas (respaldos) a la aplicación. La aplicación envía las transacciones y las firmas al servicio de pedidos, que crea un lote o bloque de transacciones y las entrega a los pares comprometidos (IBM, 2022). Cuando un par de compromisos recibió una serie de transacciones, para cada transacción válida, que se cumplió con la estrategia de copia de seguridad y verificando los lectores / registros para detectar transacciones de conflicto. Si se aprueban ambas verificaciones, el bloque se establece en el libro mayor y las actualizaciones de estado de cada transacción se reflejan en la base de datos de estado (IBM, 2022).

1.3.11. Lenguajes de Programación

a) Java

Java es más que un lenguaje, es decir, Java es una plataforma de software por su característica de Java Máquina Virtual (VM) que simula una computadora en software, la cual puede correr en diferentes computadoras y sistemas operativos, o en un hardware

diseñado específicamente para Java. El software desarrollado en Java es inherentemente cross-platform, ya que puede correr en cualquier sistema con Java VM. Una máquina virtual es en realidad otra pieza de software que interpreta y ejecuta programas Java. Esta máquina virtual requiere un código especial llamado bytecode que se almacena en un archivo llamado archivo de clase. Este código no contiene instrucciones relacionadas con la plataforma. Hay máquinas virtuales para cada plataforma porque las máquinas virtuales están programadas para una máquina específica(Becerril, 1999).

b) C++

Es un lenguaje de programación orientado a objetos (POO) genérico creado como una extensión del lenguaje de programación C o "C con clases". Los desarrolladores pueden usarlo para tareas de alto y bajo nivel, lo que les brinda a los programadores un amplio acceso al hardware en sí. C contiene varios operadores, como operadores de comparación, aritmética, manipulación de bits y lógicos. Este lenguaje de programación se usa comúnmente en gráficos por computadora y similares. Una de las mejores características es permitir que ciertos operadores estén sobrecargados. Otra característica interesante es que tiene un conjunto de clases predefinidas que son tipos de datos(Medium, 2019).

c) Solidity

Es un lenguaje de programación dealto nivel y a la vez simple que es popular entre los desarrolladores de Ethereum, y su configuración es similar a Javascript. El lenguaje está diseñado y compilado en código de bytes que es usado para crear máquinas virtuales y contratos inteligentes. Solidity es un lenguaje de programación completo de Turing para contratos. Este concepto

fue inventado por Alan Turing y se refiere a un lenguaje informático cuya potencia informática es equivalente a la llamada "máquina universal de Turing"(Medium, 2019).

d) Python

Es un lenguaje de programación de alto nivel que se interpreta en tiempo de ejecución. El proceso de ejecutar un programa en Python es similar al de cualquier otro programa. Es decir, las instrucciones de alto nivel se compilan primero en lenguaje ensamblador. En este caso, se denomina bytecode, que es una instrucción específica de Python que es interpretada en tiempo de ejecución (programada por el usuario) por un programa intérprete (la implementación de Python más utilizada) escrito en C. Como lenguaje de interpretación, no funciona tan bien como un lenguaje de interpretación que no utiliza comandos en tiempo de ejecución (SANNER, 1975).

1.3.12. Interoperabilidad

La interoperabilidad describe la medida en que los sistemas y dispositivos pueden intercambiar datos e interpretar esos datos compartidos. Para que dos sistemas sean interoperables, deben ser capaces de intercambiar datos y, posteriormente, presentar esos datos de modo que puedan ser entendidos por un usuario.(*Interoperabilidad e Intercambio de Información de Salud | HIMSS*, n.d.)

Según la (RAE, n.d.): “Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos”.

Según (Rojas et al., 2011), los diferentes tipos de interoperabilidad son los siguientes:

a. Sintáctica, se centra en definir la sintaxis de construcción de los mensajes que utilizan los sistemas de información para intercambiar datos.
b. Organizativa, se basa en la definición de las reglas de la empresa y los procedimientos operativos que regulan la participación de los distintos sujetos en los procesos de una organización.
c. Semántica, para la interpretación uniforme de los datos intercambiados, transmitidos o recibidos. De esta forma, cada sistema puede integrar la información recibida en su propia base de datos sin análisis ni procesamiento.

1.3.13. Seguridad de la información

Seguridad de la información: conjunto de precauciones y respuestas de los sistemas organizativos y tecnológicos que pueden proteger la información que busca mantener la disponibilidad, confidencialidad e integridad de los datos(Dios et al., 2017).

Este concepto solo se refiere a la seguridad de su entorno de red y no debe confundirse con el concepto de seguridad de la red. La información se puede encontrar en una variedad de medios o formatos, no solo en medios de red(Dios et al., 2017).

Es importante señalar que cuando se trata de seguridad de la información, es importante reconocer que la gestión se basa en la tecnología y puede ser información sensible. La información está centralizada y es muy valiosa. Pueden ser revelados, robados, robados, borrados o falsificados. Esto afecta su disponibilidad y lo pone en riesgo. La información es poder y se clasifica de la siguiente manera en función de las capacidades estratégicas proporcionadas por un derecho de acceso a la información en particular(Dios et al., 2017):

a) Crítica: porque para la operación de la empresa es indispensable.
b) Sensible: porque las personas autorizadas deben conocerlas
c) Valiosa: porque es muy valioso y es activo de la empresa.

El estándar ISO / IEC 27002, brinda recomendaciones para cualquier persona que esté interesada en el sistema de gestión de seguridad de la información, así como mejores prácticas en la gestión de seguridad (Arturo de la Torre et al., 2017). La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)"(ISO/IEC, 2013).

El estándar de 2013 describe las siguientes áreas clave y soluciones que deben seguirse para una implementación exitosa:

1) Políticas de Seguridad. – las directrices son(Dios et al., 2017).

   Métricas:

   a) Cobertura de las políticas, es el porcentaje de las secciones de la ISO, sobre las políticas y sus normas , los procedimientos y las directrices asociadas(Dios et al., 2017).
2) Organización de seguridad de la información. Esto incluye organizaciones internas. (Dios et al., 2017).

   Métricas:

   a) Es el porcentaje de unidades funcionales / organizacionales donde se tiene una estrategia para controlar los riesgos de seguridad por debajo del umbral(Dios et al., 2017).

b) Es el porcentaje de empleados que han aceptado el rol y las responsabilidades de seguridad de información (Dios et al., 2017).

3) Seguridad de los recursos humanos. Esto incluye cosas a considerar antes, durante y para cambios al final o cambio de trabajo. Antes de contratar, le recomendamos que investigue los antecedentes del candidato y revise los términos y condiciones. Al contratar, se recomienda abordar cuestiones relacionadas con las responsabilidades de gestión, la conciencia de seguridad de la información, la educación y la formación. En caso de despidos o cambios de trabajo, también se deben tomar medidas de seguridad como deshabilitar o renovar privilegios o derechos de acceso(Dios et al., 2017).

Métricas:

a) El porcentaje de empleados nuevos o falsos (subcontratistas, consultores, empleados temporales, etc.) se verifica y aprueba completamente de acuerdo con la política de la empresa antes de comenzar a trabajar(Dios et al., 2017).

4) En este apartado, la responsabilidad patrimonial, la clasificación de la información y la gestión de los medios de almacenamiento la gestión de dispositivos móviles, vehículos descartados y en tránsito (Dios et al., 2017).

Métricas:

a) Es el porcentaje en cada fase del proceso de clasificación los activos de información (Dios et al., 2017).

b) Es el porcentaje de activos de información con estrategias integrales implementadas para mitigar los riesgos de

seguridad de la información según sea necesario(Dios et al., 2017).

5) Control de Accesos. – Si cumplen con los requisitos organizativos de control de acceso (Dios et al., 2017).

Métricas:

a) La proporción de aplicaciones y sistemas empresariales para los que se ha identificado al "propietario" apropiado es formalmente responsable, ejecutado o aprobado para la seguridad de acceso a las aplicaciones basada en el riesgo y la evaluación y el control de acceso basado en roles en las definiciones de políticas(Dios et al., 2017).

6) Cifrado. – se refiere al control de claves y políticas de cifrado de datos(Dios et al., 2017).

Métricas:

a) Es el porcentaje que se han implantado de controles criptográficos apropiados a los datos valiosos o sensibles (Dios et al., 2017).

1.3.14. Privacidad

En el contexto de las actividades en línea, la seguridad y la privacidad de la información personal están asociadas con algunos problemas críticos como la no autorización de acceso a la información personal o la exposición no deseada de datos privados que conducen a tener algunos efectos en la privacidad del consumidor con respecto a este acceso ilegítimo(Nam, 2006).

Muchos autores han propuesto requisitos y recomendaciones para las métricas de privacidad. Por ejemplo, (Alexander et al., 2003)

requieren que las métricas de privacidad sean comprensibles para los laicos matemáticamente inclinados, sean ortogonales a las métricas de costo y utilidad, y brinden límites sobre cuán efectivamente el adversario puede tener éxito en la identificación de individuos. (Andersson & Lundin, 2008) requieren que las métricas de privacidad se basen en probabilidades (por ejemplo, la probabilidad de que un adversario identifique a un individuo determinado) y que tengan puntos finales bien definidos e intuitivos. Argumentan que una métrica debe medir la privacidad en función del número de personas que un adversario no puede distinguir y cuán uniformemente se extienden las conjeturas del adversario.

A. Dominios de privacidad

Los dominios de privacidad son áreas donde se pueden aplicar tecnologías de mejora de la privacidad (PET). Con el uso creciente de la tecnología de la información, los PET se están investigando en un número creciente de dominios. Describimos seis dominios para proporcionar contexto y ejemplos para el resto del documento(Wagner & Eckhoff, 2018).

1) Sistemas de comunicación

El principal desafío de privacidad en los sistemas de comunicación es la comunicación anónima, cuyo objetivo es ocultar qué (o incluso eso) dos usuarios se comunicaron, no solo el contenido de su comunicación. Mantener la confidencialidad de los contenidos de comunicación es un problema ortogonal que se puede resolver mediante el cifrado de clave pública(Chaum, 1988). Los adversarios generalmente intentan identificar al remitente de un mensaje, su receptor o las relaciones entre remitente y receptor(Kelly et al., 2008).

2) Bases de datos

Hay dos escenarios típicos en el dominio de la base de datos: en la configuración interactiva, los usuarios emiten consultas a una base de datos; En el entorno no interactivo, se libera una base de datos desinfectada al público. En ambos escenarios, los adversarios intentan identificar a las personas en la base de datos y revelar atributos sensibles, por ejemplo, información de salud contenida en un registro del paciente. Las bases de datos pueden incluir microdatos (es decir, información sobre individuos) o datos agregados que enmascaran información sobre individuos, por ejemplo, presentando solo los promedios de múltiples valores(Wagner & Eckhoff, 2018).

3) Servicios basados en la ubicación

Los servicios basados en la ubicación brindan servicios contextuales a los usuarios móviles, como información sobre puntos de interés cercanos. Los adversarios con acceso a información de ubicación pueden inferir atributos confidenciales como ubicaciones de hogar y trabajo, y crear perfiles de movimiento que pueden venderse o usarse con fines de marketing(Wagner & Eckhoff, 2018).

4) Medición inteligente

Los medidores inteligentes registran datos de consumo de electricidad de grano fino en la casa de un usuario y envían estos datos al proveedor de energía. El proveedor de energía puede usar estos datos para la facturación y la optimización de la red, pero también puede actuar como un adversario que infiere perfiles de comportamiento más allá del propósito establecido(Zeadally et al., 2013).

5) Redes sociales

Las redes sociales permiten a los usuarios compartir actualizaciones sobre su vida diaria. Los adversarios en este dominio intentan identificar a los usuarios en gráficos sociales anónimos, o inferir atributos sensibles de perfiles privados(Yang et al., 2012).

6) Privacidad del genoma

Los avances en la secuenciación del genoma completo han generado nuevas preguntas con respecto a la privacidad del genoma de una persona. El genoma identifica de manera única a un individuo y al mismo tiempo revela información altamente sensible, como la susceptibilidad a enfermedades. Un adversario con acceso a datos genómicos podría incurrir en discriminación genética (por ejemplo, denegación de seguro) o chantaje (por ejemplo, plantar evidencia falsa en las escenas del crimen)(Wagner & Eckhoff, 2018).

B. Características de la métrica de privacidad

A pesar de su diversidad, las métricas de privacidad comparten características comunes. Aquí, describimos cuatro características que pueden clasificar las métricas de privacidad y, por lo tanto, pueden servir como una guía inicial para elegir métricas de privacidad para escenarios específicos.

1) Metas adversas

El objetivo de las métricas de privacidad es cuantificar el nivel de privacidad en un sistema o la privacidad proporcionada por un PET, a menudo bajo la consideración de un adversario específico. El adversario tiene como objetivo comprometer la privacidad de los usuarios y

aprender información confidencial. Esta información confidencial puede ser identidades de usuario (por ejemplo, desanonizando conjuntos de datos), propiedades del usuario (por ejemplo, ubicación o consumo de energía), o ambos(Heurix et al., 2015). Por lo tanto, es importante seleccionar métricas que puedan medir el aspecto relevante. Por ejemplo, una métrica en los servicios basados en la ubicación puede indicar si el adversario puede identificar a un usuario, dada una ubicación (ocultación de identidad), o si el adversario puede identificar la ubicación, dado un usuario (ocultación de propiedad)(Wagner & Eckhoff, 2018).

2) Capacidades Adversarias

Naturalmente, un adversario más fuerte, como uno con más recursos o conocimiento previo, podría atacar la privacidad con más éxito. El valor de una métrica de privacidad, por lo tanto, depende del modelo adversario, y evaluar un PET con un modelo adverso débil puede conducir a una sobreestimación de la privacidad. Esencialmente, los PET que brindan protección contra un modelo adversario más fuerte pueden brindar garantías de privacidad más fuertes. Como resultado, las métricas solo se pueden usar para comparar dos PET diferentes si usan el mismo modelo adversario(Wagner & Eckhoff, 2018).

Las métricas que no tienen en cuenta ningún tipo de adversario suponen implícitamente un adversario con capacidades limitadas. Por ejemplo, las métricas que miden la privacidad únicamente en función de ciertas propiedades de datos suponen que cada ataque al sistema solo dependerá de estas propiedades. Sin embargo, los ataques

que explotan otras propiedades de los datos pueden revelar información confidencial(Wagner & Eckhoff, 2018).

La literatura refleja la importancia de los modelos adversarios al considerar adversarios con diversas características. Para permitir una mejor interpretación del resultado de las métricas de privacidad, los estudios siempre deben incluir una descripción detallada del modelo de adversario utilizado. Con este fin, ampliamos la taxonomía de los tipos adversarios descritos por(Díaz et al., 2003), y clasifica a los adversarios de la siguiente manera:

a) Local – Global. Los adversarios locales solo pueden actuar en una parte restringida del sistema, por ejemplo, una ubicación geográfica o un subconjunto de nodos. Los adversarios globales tienen acceso a todo el sistema(Wagner & Eckhoff, 2018).

b) Activo – Pasivo. Los adversarios activos pueden interferir con el sistema al agregar, eliminar o modificar información o comunicación. Los adversarios pasivos solo pueden leer y observar(Wagner & Eckhoff, 2018).

c) Interno – Externo. Los adversarios internos son parte del sistema, por ejemplo, servidores que brindan servicios basados en la ubicación, proveedores de energía en medición inteligente o terceros que controlan nodos en el sistema. Los adversarios externos no son parte del sistema, pero pueden atacarlo, por ejemplo, a través de enlaces de comunicación compartidos o datos disponibles públicamente(Wagner & Eckhoff, 2018).

d) Estático – Adaptativo. Los adversarios estáticos eligen qué estrategia y recursos usar antes de un ataque y se

adhieren a su elección independientemente de cómo avance el ataque. Los adversarios adaptativos pueden adaptar su estrategia mientras el ataque está en curso, por ejemplo, aprendiendo los parámetros del sistema a través de la observación(Wagner & Eckhoff, 2018).

e) Conocimientos previos. Algunos adversarios pueden tener conocimiento adicional sobre el sistema, como conocimiento general específico del dominio - conocimiento sobre el mundo - o conocimiento específico del escenario, por ejemplo, en forma de una distribución de probabilidad previa o información específica sobre los usuarios del sistema, como sus domicilios y direcciones de trabajo. La información previa puede fortalecer considerablemente al adversario y, por lo tanto, es importante que las métricas de privacidad puedan explicarlo(Wagner & Eckhoff, 2018).

f) Recursos. Los adversarios también se pueden clasificar de acuerdo con los recursos disponibles para ellos. Para los recursos computacionales, los adversarios eficientes están restringidos a algoritmos de tiempo polinomial probabilístico (PPT), mientras que los adversarios ilimitados no están restringidos a ningún modelo computacional. Otros tipos de recursos incluyen el ancho de banda o el número de nodos maliciosos disponibles para el adversario(Murdoch, 2014).

3) Fuentes de datos

Las fuentes de datos describen qué datos deben protegerse y cómo se supone que el adversario tiene acceso a los datos.

a) Datos publicados. Los datos publicados se refieren a información que ha sido puesta a disposición voluntaria y persistentemente al público. Esto incluye bases de datos estadísticas, así como información que las personas eligen divulgar, por ejemplo, en las redes sociales. En ambos casos, los adversarios intentan identificar individuos anonimizados o revelar atributos sensibles(Wagner & Eckhoff, 2018).

b) Datos observables. Los datos observables son información transitoria que requiere que el adversario esté presente para poder acceder a ellos. Esta categoría incluye información que puede obtener un adversario pasivo que puede acceder a los datos sin comprometer el sistema subyacente. En los sistemas de comunicación, por ejemplo, los adversarios escuchan las comunicaciones para identificar a los remitentes y receptores de mensajes(Wagner & Eckhoff, 2018).

c) Datos reutilizados. Los datos rediseñados se usan para un propósito diferente al propósito para el que se adquirieron inicialmente. Algunos ejemplos son los proveedores de servicios que obtienen información del usuario para ofrecer servicios basados en la ubicación, medición inteligente o redes sociales, pero luego usan esta información para fines distintos a la prestación del servicio. Tener acceso a información de usuarios no públicos (independientemente de la configuración de privacidad de los usuarios) permite la publicidad personalizada y otras formas de comercialización o monetización(Wagner & Eckhoff, 2018).

d) Todos los demás datos. Todos los demás datos se refieren a información que no se hizo pública, no era observable y que el adversario no tenía la intención de tener acceso a ella. Por lo general, estos datos no están anonimizados ni protegidos, y pueden obtenerse utilizando métodos como escuchas telefónicas, piratería informática en un sistema, chantaje o compra en el mercado negro. Las implicaciones para los usuarios pueden ser graves, incluidas las pérdidas financieras y la publicación de registros médicos o comunicaciones confidenciales. A menudo, el propietario original no implementa las PET, ya que pueden hacer que sea menos conveniente trabajar con los datos(Wagner & Eckhoff, 2018).

4) Entradas para el cálculo de métricas

Las métricas de privacidad se basan en diferentes tipos de datos de entrada para calcular los valores de privacidad. La disponibilidad de los datos de entrada o los supuestos apropiados determinan si una métrica se puede utilizar en un escenario específico(Wagner & Eckhoff, 2018).

a) Estimación del adversario. La estimación del adversario es el resultado del esfuerzo del adversario por violar la privacidad. A menudo toma la forma de una distribución de probabilidad posterior. Por ejemplo, en un sistema de comunicación, la estimación puede describir la probabilidad de que cada usuario haya enviado un mensaje. En la medición inteligente, la estimación puede describir cuánta energía es probable que un usuario haya consumido durante un período de tiempo específico(Wagner & Eckhoff, 2018).

b) Recursos del adversario. Los recursos disponibles para el adversario se pueden proporcionar, por ejemplo, en términos de potencia computacional, tiempo, ancho de banda o nodos físicos(Wagner & Eckhoff, 2018).

c) Resultado verdadero. El verdadero resultado, o la verdad fundamental, a menudo se usa para juzgar qué tan buena es la estimación del adversario. Sin embargo, esta información no está disponible para el adversario, por lo que no puede calcular las métricas que utilizan el resultado real. Por ejemplo, en los servicios basados en la ubicación, el verdadero resultado corresponde a la verdadera ubicación de un usuario, y en las redes sociales corresponde a las verdaderas conexiones en un gráfico social. Se suele suponer que la verdad básica describe datos confidenciales(Wagner & Eckhoff, 2018).

d) Conocimientos previos. El conocimiento previo describe el conocimiento concreto y específico del escenario que tiene el adversario. Por lo general, toma la forma de una distribución de probabilidad previa. En la privacidad del genoma, por ejemplo, el conocimiento previo puede incluir información sobre el grupo de población de un usuario, lo que influye en la probabilidad de que un usuario tenga variaciones genéticas específicas(Wagner & Eckhoff, 2018).

e) Parámetros. Los parámetros configuran métricas de privacidad. Describen valores umbral, la sensibilidad de los atributos, qué atributos son sensibles o los niveles de privacidad deseados(Wagner & Eckhoff, 2018).

5) Medidas de salida

El resultado de una métrica de privacidad se refiere al tipo de propiedad que mide una métrica de privacidad. Introducimos una taxonomía con ocho propiedades de salida, cada una de las cuales representa un aspecto diferente de la privacidad. Esta es una categorización importante porque muestra que una sola métrica no puede capturar todo el concepto de privacidad. Una estimación más completa de la privacidad solo se puede obtener mediante el uso de métricas de diferentes categorías de salida(Wagner & Eckhoff, 2018).

a) Incertidumbre. Las métricas de incertidumbre suponen que una alta incertidumbre en la estimación del adversario se correlaciona con una gran privacidad, porque el adversario no puede basar sus conjeturas en información conocida con certeza. Sin embargo, incluso las suposiciones basadas en información incierta pueden ser correctas y, por lo tanto, los usuarios individuales pueden sufrir pérdidas de privacidad incluso en escenarios con un adversario altamente incierto(Wagner & Eckhoff, 2018).

b) Ganancia o pérdida de información. Las métricas que miden la ganancia o pérdida de información cuantifican la cantidad de información obtenida por el adversario, o la cantidad de privacidad perdida por los usuarios debido a la divulgación de información(Wagner & Eckhoff, 2018).

c) Similitud de datos. Las métricas de similitud de datos miden la similitud dentro de un conjunto de datos, por ejemplo, formando clases de equivalencia, o entre dos conjuntos de datos, por ejemplo, entre un conjunto de datos privado y su contraparte pública y desinfectada.

Estas métricas se abstraen de un adversario y se centran en las propiedades de los datos. Por ejemplo, la similitud puede referirse a las frecuencias de los valores de los datos, la similitud numérica o la (falta de) variación en los datos publicados(Wagner & Eckhoff, 2018).

d) Indistinguibilidad. La indistinguibilidad es una noción clásica en la comunidad de seguridad. Las métricas basadas en la indistinguibilidad analizan si el adversario puede distinguir entre dos resultados de un mecanismo de privacidad. La privacidad es alta si el adversario no puede distinguir entre ningún par de resultados. Las métricas en esta categoría son generalmente binarias; indican si dos resultados son indistinguibles o no, pero no cuantifican los niveles de privacidad intermedios(Wagner & Eckhoff, 2018).

e) Probabilidad de éxito del adversario. Las métricas que utilizan la probabilidad de éxito del adversario para cuantificar la privacidad indican la probabilidad de que el adversario tenga éxito en un solo intento, o con qué frecuencia tendrían éxito en un gran número de intentos. Las bajas probabilidades de éxito se correlacionan con una alta privacidad. Si bien esta suposición es válida para una población promedio de usuarios, un usuario individual puede sufrir una pérdida de privacidad incluso cuando la probabilidad de éxito del adversario es baja(Wagner & Eckhoff, 2018).

f) Error. Las métricas basadas en errores miden cuán correcta es la estimación del adversario, por ejemplo, utilizando la distancia entre el resultado real y la estimación. Alta corrección y pequeños errores se

correlacionan con baja privacidad(Wagner & Eckhoff, 2018).

g) Tiempo. Las métricas basadas en el tiempo miden el tiempo hasta el éxito del adversario o el tiempo hasta la confusión del adversario. En el primer caso, las métricas suponen que el adversario tendrá éxito eventualmente, por lo que un tiempo más largo se correlaciona con una mayor privacidad. En el segundo caso, las métricas suponen que el mecanismo de privacidad eventualmente confundirá al adversario, por lo que un tiempo más corto se correlaciona con una mayor privacidad(Wagner & Eckhoff, 2018).

h) Precisión. Estas métricas cuantifican la precisión de la estimación del adversario sin considerar la corrección de la estimación. Estimaciones más precisas se correlacionan con una menor privacidad(Wagner & Eckhoff, 2018).

1.4. Formulación del Problema.

¿Cuál es el impacto de evaluar una arquitectura Blockchain MA-ABS en la gestión de historias clínicas electrónicas peruanas con respecto a la seguridad y privacidad?

1.5. Justificación e importancia del estudio.

Esta investigación se justifica en la evaluación de la arquitectura blockchain utilizando el esquema de firmado basado en atributos en múltiples autoridades (MA-ABS) en la gestión de historias clínicas electrónicas peruanas. Esta arquitectura aborda dos principales problemas destacados en la gestión de las Historias clínicas electrónicas: la privacidad de la información y seguridad de datos de los pacientes.

Esta investigación describe una alternativa de gestionar las Historias clínicas electrónicas en los centros médicos que tienen su información centralizada y pueden ser vulnerables a ataques de virus o códigos maliciosos, y también a los pacientes, debido al nivel de privacidad que tiene la arquitectura, es decir que su información solo podrá ser observada, modificada o actualizada si este lo autoriza. Además, esta instigación puede ser utilizada como ejemplo no solo en el área de salud sino también en otras áreas como el financiero, electoral, comercio, entro otros.

1.6. Hipótesis.

La evaluación de la arquitectura blockchain MA-ABS en la gestión de historias clínicas electrónicas peruanas impactará positivamente en la mejora de la seguridad y privacidad.

1.7. Objetivos.

Evaluar la arquitectura blockchain MA-ABS para gestión de historias clínicas electrónicas peruanas

Objetivos específicos

1) Seleccionar la Arquitectura Blockchain más adecuada para gestión de historias clínicas electrónicas.
2) Modelar la arquitectura Blockchain de acuerdo a la arquitectura seleccionada.
3) Seleccionar la plataforma tecnológica compatible a la arquitectura a utilizar.
4) Desarrollar una aplicación de gestión de historias clínicas utilizando arquitectura blockchain MA-ABS.
5) Realizar las pruebas a la arquitectura Blockchain implementada.

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación.

2.1.1. Tipo de investigación

Esta investigación tecnológica aplicada de tipo Cuantitativa por la recopilación y el análisis de datos para responder preguntas de la encuesta y respaldar hipótesis previamente establecidas basadas en mediciones, recuentos y uso sistemático, además de tecnológica porque como producto de este proceso investigativo se obtendrá un producto de software de gestión de historias clínicas electrónicas y será aplicada porque se ha utilizado información de artículos científicos publicados en principales journals para ser implementados y ponerlos en despliegue(Hernández Sampieri et al., 2006).

2.1.2. Diseño de la investigación:

El diseño utilizado es de tipo experimental, de acuerdo al tipo de investigación, del sub tipo cuasi experimental y será aplicada a un solo grupo porque se analizará la arquitectura blockchain manipulando de forma deliberada la variable independiente, para observar sus efectos en la variable dependiente planteada(Hernández Sampieri et al., 2006).

2.2. Población y muestra.

2.2.1. Población:

Para obtener la población en esta investigación, se debe tener en cuenta la totalidad del fenómeno a estudiar, donde las entidades que se están estudiando poseen una característica en común y da origen a los datos a esta investigación(Hernández Sampieri et al., 2006).

La población de la presente investigación contará con 17 de las diferentes arquitecturas blockchain que están en el mercado, tanto arquitecturas comerciales como las de investigación, las cuales se evaluaran mediante según sus ventajas y desventajas. La evaluación se detalla en el Anexo 01.

2.2.2. Muestra:

La muestra para esta investigación es un subgrupo de la población, y debe ser no probabilística, debido a que la selección de los elementos no depende de una probabilidad, sino a características planteadas por el investigador(Hernández Sampieri et al., 2006).

La muestra de la presente investigación está representada por una (01) arquitectura blockchain MA-ABS, y se eligió según la evaluación de la matriz de arquitectura blockchain según se muestra en el anexo 02.

2.3. Variables, Operacionalización.

Variable dependiente: Gestión de historias clínicas electrónicas peruanas.

Variable Independiente: Arquitectura Blockchain.

2.3.1. Operacionalización de Variables

Tabla 4

Operacionalización de variables dependiente e independiente del proyecto de investigación.

VARIABLES	DIMENSIONES	INDICADORES	DESCRIPCIÓN	FÓRMULA
DEPENDIENTE Gestión de historias clínicas electrónicas peruanas	Gestión	Planificación	Porcentaje obtenido del numero de tareas planificadas (NTP) sobre el total de tareas de historias clinicas electronicas (TTHCE).	$\frac{NTP}{TTHCE}$
		Ejecución	Porcentaje obtenido del numero de tareas ejecutadas (NTE) sobre el total de tareas de historias clinicas electronicas (TTHCE).	$\frac{NTE}{TTHCE}$
		Control	Porcentaje obtenido del numero de tareas controladas (NTC) sobre el total de tareas de historias clinicas electronicas (TTHCE).	$\frac{NTC}{TTHCE}$
INDEPENDIENTE Arquitectura Blockchain	Seguridad	Control de Accesos	Numero de accesos satisfactorios (NAS) según el rol correspondiente sobre el total de accesos de los usuarios (TAU).	$\frac{NAS}{TAU}$
	Privacidad	Ganancia o pérdida de información	El número de usuarios comprometidos (NUC) con su información sobre total de usuarios (TU)	$\frac{NUC}{TU}$

Fuente: Elaboración propia.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

2.4.1. La observación

La observación es una técnica que nos va a ser de utilidad en el análisis del progreso de la investigación, pues se basa en la observación de determinados individuos en el momento que desempeñan una tarea.

En lo que respecta a esta investigación la observación es directa al comportamiento del prototipo de Gestión de Historias Clínicas Electrónicas para establecer la correlación respecto a la seguridad y privacidad.

2.4.2. Análisis documental

Medios impresos, se analizará los formatos de las historias clínicas y las normativas para su gestión de acuerdo a reglamentos y leyes peruanas.

2.4.3. Ficha de observación

Según la técnica de observación se elaborará fichas de observación para registrar la información observada.

2.5. Procedimiento de análisis de datos

Se utilizó el método de la observación para la recolección de datos, el método empieza desde la formulación del problema para poder organizar los objetivos y las variables que resulten relevantes, luego se tiene la recolección de datos, los cuales servirán para probar la hipótesis; una vez obtenidos los datos se procederá al análisis e interpretación de los datos observados a las pruebas del software de gestión de historias clínicas electrónicas, que se deberán plasmar en tablas y gráficos estadísticos, y por ultimo tenemos la comunicación de resultados que estarán redactados en

las conclusiones del trabajo y servirán para estimular e inspirar a otros investigadores a la continuación del tema.

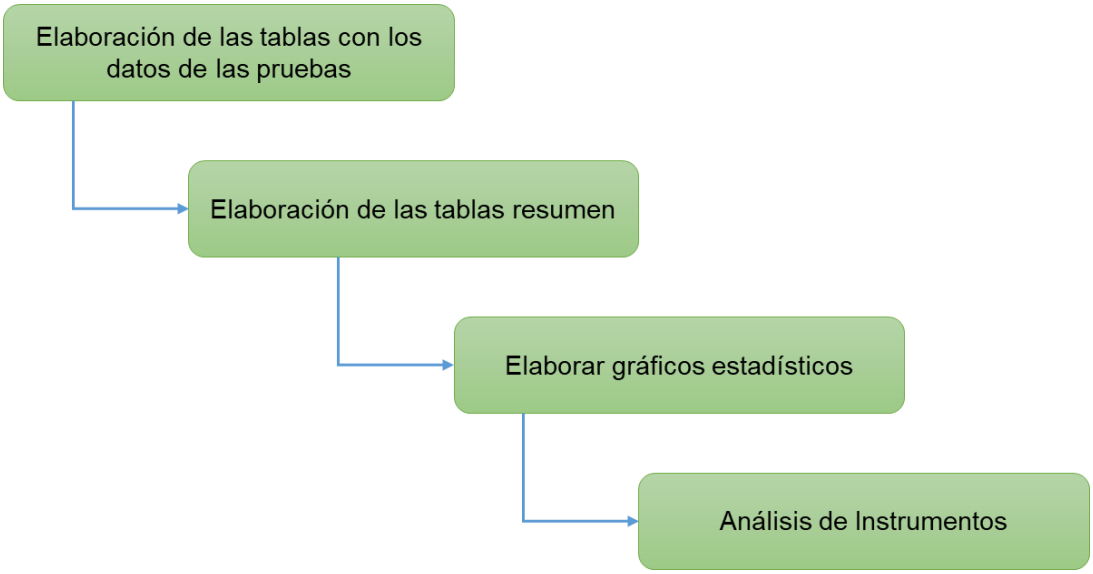


Figura 15. Enfoque propuesto para el desarrollo del proyecto de investigación. Fuente: Elaboración propia

2.6. Criterios éticos.

2.6.1. El consentimiento informado

Uno de los principios éticos más importantes es el consentimiento informado que representa que el alumno garantice voluntariamente su intención de participar en la investigación, habiendo antes comprendido la información que se le ha otorgado.

2.6.2. La confidencialidad

La confidencialidad se define como la garantía de que la información brindada sea protegida y no divulgada sin consentimiento del sujeto.

Esta garantía se lleva a cabo mediante reglas que limitan el acceso a esta información.

2.6.3. Manejo de riesgos

El manejo de riesgos engloba dos aspectos principales que son: Primero, el investigador tiene que cumplir cada una de las responsabilidades y obligaciones adquiridas con los informantes, y segundo se refiere al manejo posterior de los datos que se han proporcionado.

2.7. Criterios de Rigor Científico

2.7.1. Consistencia

El trabajo actual mantiene la coherencia y la eficiencia de los datos, y el análisis de la aplicación de datos se realiza en la mayor medida posible utilizando habilidades, competencias y conocimientos en ingeniería e investigación.

2.7.2. Validez

Los resultados de este estudio serán evaluados y analizados a fondo para obtener resultados útiles que ayuden a resolver las cuestiones planteadas.

2.7.3. Fiabilidad

La investigación sigue este principio al obtener resultados similares a los propuestos originalmente, utilizando una variedad de técnicas y herramientas de medición aplicables a la recolección y transformación de información.

2.7.4. Transferibilidad

Este estudio proporciona información y conocimientos que se pueden impartir a los investigadores que se centran en situaciones similares.

2.7.5. Neutralidad

La forma en que se desarrolla la investigación asegura que los resultados obtenidos no sean alterados o secuestrados por las motivaciones, preferencias y / u opiniones del investigador.

III. RESULTADOS

3.1. Resultados en Tablas y Figuras

Para evaluar los indicadores de privacidad y seguridad en la implementación de la arquitectura Blockchain planteada.

La privacidad de la información, debe validar que la información guardada por un usuario, debe ser la misma que se muestre a otro usuario.

Tabla 5

Tareas completadas para el indicador de privacidad.

Tareas	Tareas completadas	Porcentaje (%)
Tarea 1	20	0%
Tarea 2	20	0%

Fuente: Elaboración Propia

Para evaluar el indicador de privacidad, se utilizó la métrica de pérdida o ganancia de información, donde al ejecutar las tareas desarrolladas por el medico (tarea 1) y las tareas del paciente (tarea 2), se obtiene un 0% de perdida de información, esto quiere decir que la información enviada por la tarea 1 es la misma que se muestra en la tarea 2.

Figura 16. Cuadro estadístico para el indicador de privacidad

Fuente: Elaboración Propia.

La seguridad de los datos, se debe evaluar mediante el control de acceso en una aplicación, donde se valida que la tarea realizada por el paciente al consultar su historia clínica, verifique la clave pública y privada para acceder a la red creada en Blockchain. Donde se desarrolló una tarea solo por el paciente (tarea 1), dando como resultado un 100%.

Tabla 6

Tareas completadas para el indicador de seguridad.

Tareas	**Tareas completadas**	**Porcentaje (%)**
Tarea 1	20	100%

Fuente: Elaboración Propia

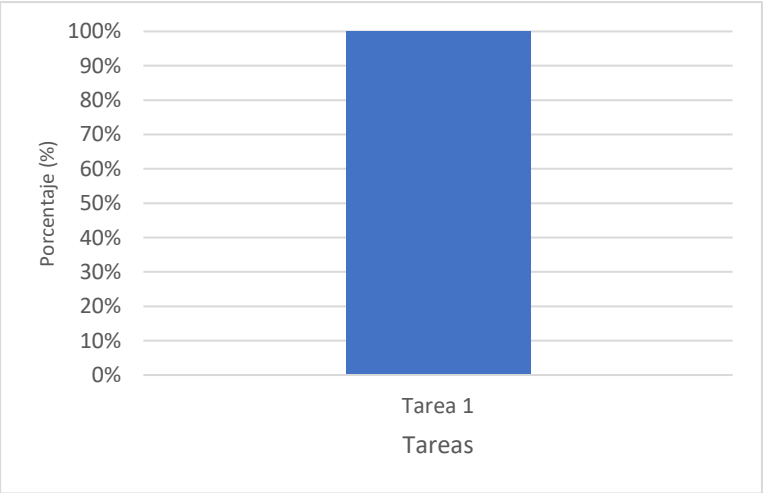


Figura 17. Cuadro estadístico para el indicador de seguridad

Fuente: Elaboración Propia.

3.2. Discusión de resultados

Como objetivo general se consideró evaluar la arquitectura blockchain MA-ABS para gestión de historias clínicas electrónicas peruanas, en base a ello se realizaron pruebas en relación a los indicadores de privacidad de información con su métrica ganancia o pérdida de información, y de seguridad de datos con su métrica de control de acceso.

En los resultados obtenidos en la presente investigación, al realizar pruebas a los pacientes y médicos mediante la aplicación desarrollada según las características de la arquitectura Blockchain, se observó que el 100% de las tareas realizadas para el indicador de privacidad de información se obtuvo un 0% de perdida de información, y para el indicador de seguridad se obtuvo un 100% en el control del acceso al consultar la historia clínica del paciente.

Los resultados obtenidos en la presente investigación, no se pudieron comparar o contrastar con otras investigaciones, debido que, al momento de realizar la presente investigación, no se encontraron artículos o investigaciones similares.

La arquitectura Blockchain MA-ABS para la gestión de historias clínicas electrónicas peruanas, si brinda la privacidad de información y la seguridad de los datos.

3.3. Aporte práctico

Para seleccionar la arquitectura de esta investigación, se realizó los siguientes pasos como se muestra en la Figura 18:

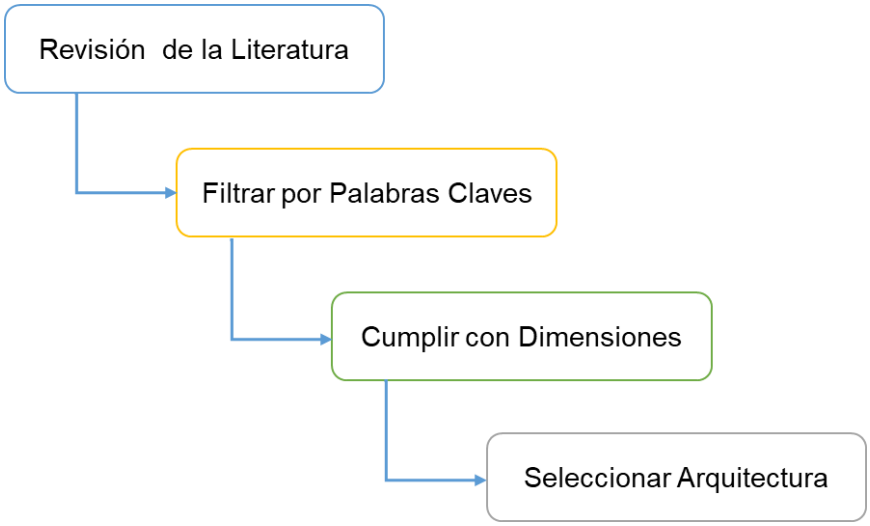


Figura 18. Enfoque propuesto para la selección de la Arquitectura Blockchain más adecuada. Fuente: Elaboración Propia.

Primero se realizó una revisión de las literaturas científicas publicadas en diferentes journals reconocidos a nivel mundial y que albergan una gran cantidad de artículos en su base de datos como IEEE Xplore Digital Library, ScienceDirect y MDPI donde se utilizó palabras claves como se puede apreciar en la Tabla 7 donde se encontró 200 artículos científicos.

Tabla 7

Resultado de la búsqueda en los journals

N°	Journal	Regla de Búsqueda	Resultado
1	IEEE Xplore Digital Library	(((((Blockchain) AND electronic medical records) AND privacy) AND security) AND healthcare)	24
2	ScienceDirect	(((((Blockchain) AND electronic medical records) AND privacy) AND security) AND healthcare)	63
3	MDPI	(((Blockchain) AND records) AND healthcare)	113

Fuente: Elaboración propia.

De dichos artículos, se encontraron 17 arquitecturas blockchain propuestas las cuales se muestran en la Tabla 8, dichas arquitecturas se verificaron si cumplen

con las dimensiones que se está investigando en este informe como la seguridad y privacidad. Mediante dicho análisis se escogió a la arquitectura Blockchain MA-ABS para implementar en la presente investigación, debido que presenta como ventaja la seguridad en los datos y preserva la privacidad.

Tabla 8

Arquitecturas Blockchain propuestas con las dimensiones de Seguridad y Privacidad

N°		Año	Autor(es)	Seguridad	Privacidad
1	MedRec	2018	Guo et al.	SI	SI
2	Healthcare Data Gateways	2019	Al-Karaki et al.	SI	SI
3	Stony Brrok Study	2019	Nortey et al.	NO	SI
4	Pati entory	2019	Kassab et al.	NO	SI
5	Modum.io AG	2019	Rajput et al.	SI	SI
6	TMSMD	2019	Chen et al.	SI	NO
7	MeDShare	2018	Vora et al.	NO	SI
8	MedRec 2.0	2019	Zaghloul et al.	SI	SI
9	Medical Chain	2018	Liu et al.	SI	SI
10	Smart Contracts for Wearables	2019	Nguyen et al.	SI	SI
11	Identity and Access Management	2019	Huang et al.	SI	SI
12	PBE - DA	2018	Xiao et al.	SI	SI
13	Clinical Trials Monitoring	2019	Yovera-Loayza et al.	NO	SI
14	Blockchain-based Digital Health Information Exchange	2016	Azaria et al.	NO	SI
15	MA-ABS	2019	Guo et al.	SI	SI
16	Ancile	2017	Alhadhrami et al.	NO	SI
17	MediBChain	2019	de Oliveira et al.	SI	SI

Fuente: Elaboración propia.

La arquitectura MA-ABS propuesta garantiza la eficiencia de los EHR encapsulados en la cadena de bloques, lo que permite a los pacientes aprobar notificaciones en función de sus atributos sin revelar ninguna información que no sea una prueba de sí mismos. También existe una única autoridad central o no confiable que puede generar y distribuir las claves públicas / privadas de los pacientes, evitando así problemas de custodia y cumplimiento con los regímenes de retención de datos de blockchain distribuidos. Con el sistema blockchain HCE, varias organizaciones se

unen a ABS para introducir el sistema MA-ABS para proteger la privacidad del paciente. Esto asegura el anonimato de la información que cumple con los requisitos de la estructura de la cadena de bloques.

Una vez elegida la Arquitectura Blockchain, se verificó sus características y componentes para modelar la arquitectura, este modelo de sistema de Historias Clínicas Electrónicas -HCE se constituyó de las siguientes cuatro partes: un servidor de HCE, autoridades N, pacientes y verificadores de datos. Como se muestra en la Figura 19, el servidor de HCE es como un servidor de almacenamiento en la nube, que es responsable de almacenar y transmitir las HCE. Las autoridades N son varias organizaciones diferentes, como hospitales, organizaciones de seguros médicos, institutos de investigación médica, etc., que son responsables de aceptar la inscripción y el intercambio de información de pacientes. Los pacientes pueden crear, gestionar, controlar y firmar sus propios registros médicos electrónicos y definir el predicado mientras que el verificador de datos puede acceder a esta firma y verificar la exactitud.

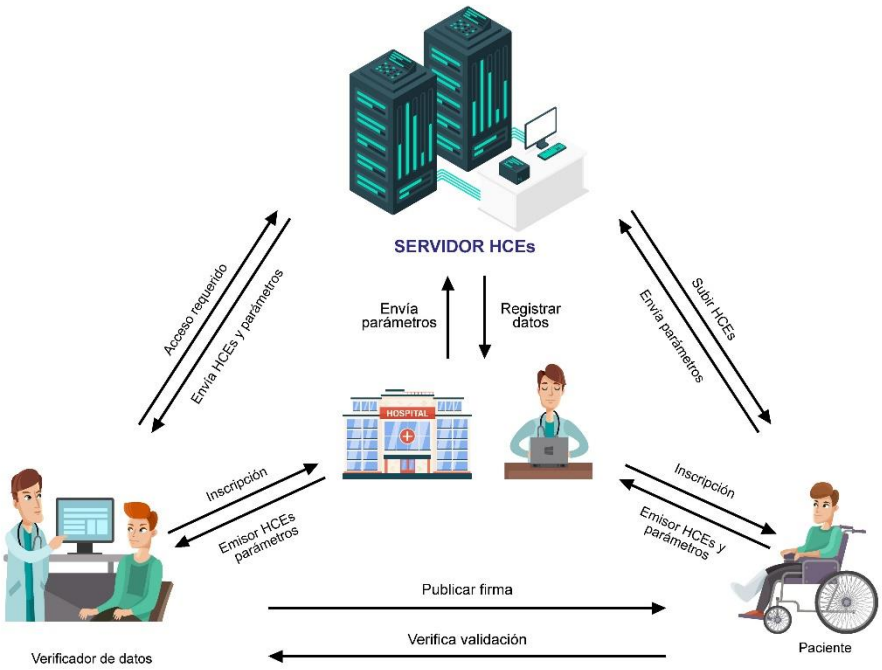


Figura 19.

Modelo formado de cuatro partes: servidor de EHR, autoridades, paciente y verificador de datos. Fuente: (Guo et al., 2018).

El sistema de HCEs con una estructura de cadena de bloques se diseña como se muestra en la Figura *20*. Cada paciente posee una cadena de bloques de atención médica únicamente. Después de recibir tratamiento en un hospital, toda la información, incluidas las HCE, los registros de consumo, los registros de seguros, etc., se resume en un bloque. Los tratamientos de los pacientes en diferentes momentos se generarán en diferentes bloques. Luego, se construye una serie de bloques generados de acuerdo con la secuencia de tiempo y un blockchain sanitario de este paciente.

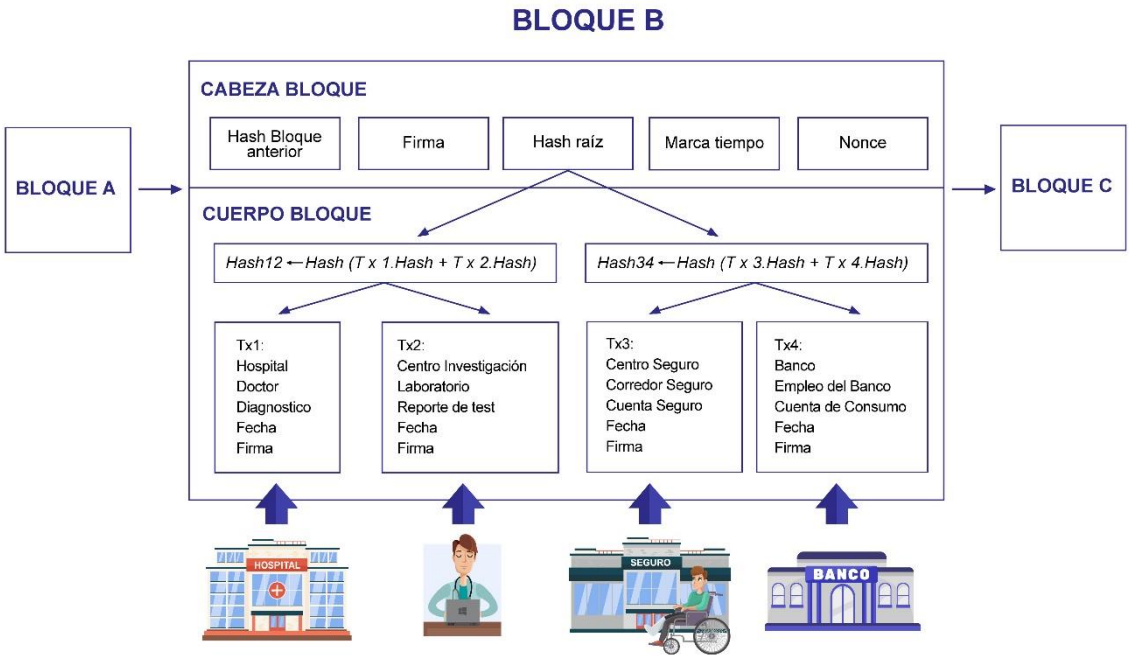


Figura 20. Sistema de cadena de Bloques del sistema HCEs. Fuente: (Guo et al., 2018).

Para seleccionar la plataforma tecnológica se realizó una búsqueda de las diferentes plataformas que existen actualmente, donde se encontraron 12, como se muestra en la Tabla 9, que mediante una comparación de si cuentan con un contrato inteligente, si utilizan tokens, que mecanismo de consenso tienen, el Lenguaje de Programación y en qué sistema operativo se puede implementar, además de buscar a los proveedores de Blockchain que actualmente brindan este servicio como se muestra en la Tabla 10, se eligió a la plataforma tecnológica

Hyperledger Fabric y al proveedor IBM Blockchain plataforma, por ser una plataforma abierta, interoperable y disponible para cualquier empresa.

Tabla 9

Comparación de Plataformas Tecnológicas de Blockchain

	Contratos inteligentes	**Creación de tokens**	**Mecanismo de consenso**	**Leguaje de programación**	**SO**
Hyperledger	Si	Si	PoET	Pyton, Go, Rust, Java, C++	Windows, Linux
Ethereum	Si	Si	PoW	Go, C++, Rust, Pyton, Java	Windows, Linux, Mac, Android, IOS
Quorum	Si	Si	PoW	Go, Java	Windows, Linux
MultiChain	No	Si	PoW	Pyton, C#, Ruby	Windows, Linux, Mac
Eris	Si	Si	PoW	Go	Linux, Windows, Mac
Cardano	Con restricciones	Con restricciones	PoS	Haskell	Windows, Mac
Komodo	Si	Si	PoW, dPoW	C++, C	Windows, Linux, Mac, Android, IOS
Chain Core	Si	Si	PoA	C++, Go	Windows
Corda	Si	Si	Raft	Kotlin, Java	Windows, Mac
Ripple	Si	Si	RPCA	C++	Windows, Linux, Mac
Waves	Si	Si	LPoS	Scala	Windows, Linux, Mac, Android, IOS
Ardor	Con restricciones	Si	PoS	Java	Windows, Linux, Mac, Android, IOS

Fuente: Elaboración Propia

Tabla 10

Comparación de proveedores Blockchain como servicio

Proveedores Blockchain	Plataforma	Escalable y Seguro	Fiabilidad	Prueba Gratuita
Amazon	Hyperledger Fabric	SI	SI	NO
Microsoft (Azure)	Ethereum, Hyperledger Fabric	SI	SI	NO
IBM	Hyperledger Fabric	SI	SI	SI
Oracle	Hyperledger Fabric	SI	SI	NO

Fuente: Elaboración Propia

Para realizar la aplicación de gestión medica de historias clínicas se debe tener en cuenta el proceso que tiene un paciente para realizar una cita médica, como se muestra en la Figura 21, donde el paciente primero debe ingresar al aplicativo y buscar a un especialista, una vez seleccionado debe elegir si él o un familiar es el que se va a atender, luego elegir una fecha disponible para que se guarde la cita, el paciente podrá cancelar la cita si lo desea, una vez generada la cita, el medico recibirá la cita y procederá a realizar la consulta, al terminar el paciente podrá realizar una opinión y finalizará registrando la cita en la Historia Clínica del paciente.

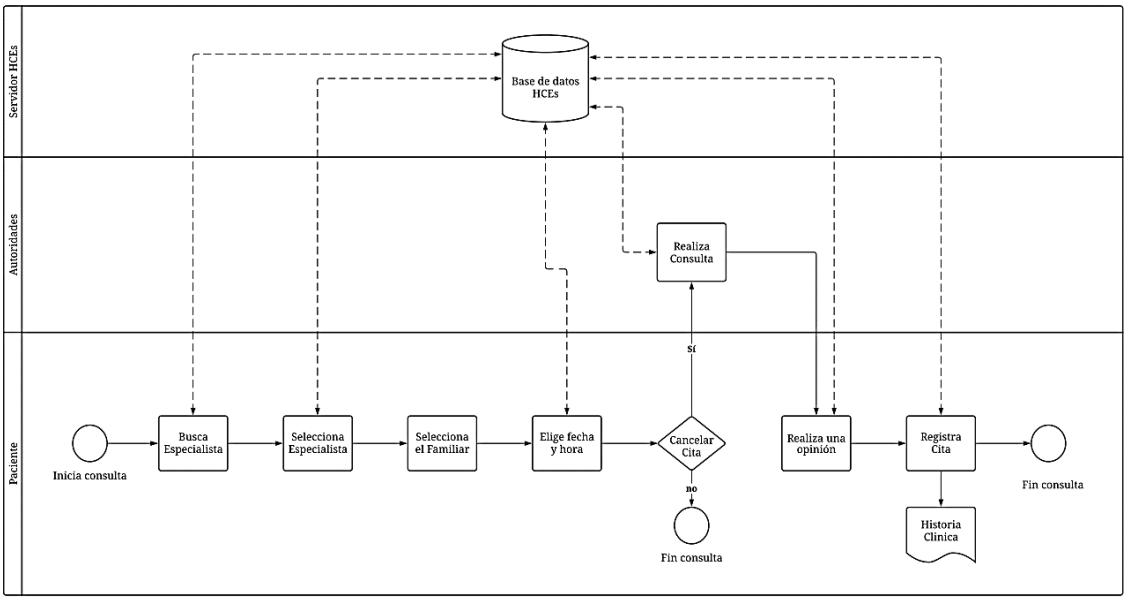


Figura 21. Diagrama de procesos de una atención medica relacionado al paciente
Fuente: Elaboración Propia

La aplicación se desarrolló mediante los mockups que se muestran en las figuras siguientes, interfaces de inicio de sesión, donde el paciente, el doctor o el administrador de la aplicación podrán iniciar sesión y serán redirigidos mediante su rol correspondiente.

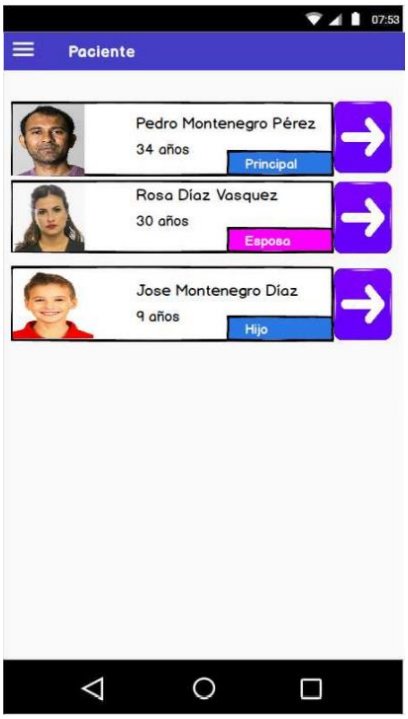
Figura 22. Mockup de inicio de sesión del paciente, médico o administrador
Fuente: Elaboración propia

Los siguientes mockups permiten al paciente tener una lista de las distintas especialidades registradas, donde podrá elegir y se mostraran los distintos especialistas según dicha especialidad. Una vez seleccionado el especialista se mostrarán sus datos generales y se podrá dar clic para empezar la cita médica. Se deberá elegir si es el paciente o uno de sus familiares el que realizará la cita y se deberá elegir una fecha y hora disponible, agregando una descripción de la cita.

a.

b.

c.



d.

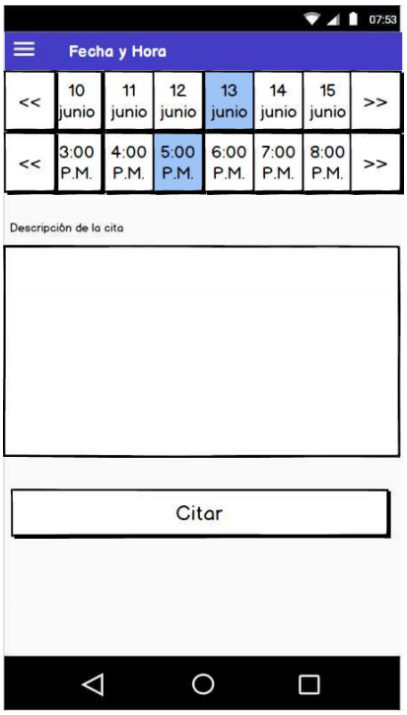


Figura 23. Mock up de la vista del paciente a. Selección de especialidades, b. Selección de especialistas, c. Selección de un familiar, d. Selección de fecha y hora disponible. Fuente: Elaboración Propia

La aplicación se realizó mediante la metodología de desarrollo ágil scrum, el back-end en el framework Laravel 8, debido a que es simple y es uno de los framework más utilizados y de mayor comunidad en el mercado y el Front-end en Flutter, ya que es una interfaz de usuario expresiva y flexible, utilizando el manejador de base de datos Mysql, requerido por la utilización de un servicio host, para el almacenamiento de los datos.

La aplicación cuenta con los siguientes requerimientos funcionales:

Tabla 11.

Requerimientos funcionales de la aplicación

N	Requerimiento	Descripción
1	Iniciar sesión mediante correo y contraseña.	El sistema deberá permitir el inicio de sesión mediante correo y contraseña.
2	El paciente podrá registrar a un familiar en su grupo familiar	El registro deberá permitir el registro de los familiares del paciente.
3	El paciente podrá ver un listado de su grupo familiar	El sistema deberá permitir visualizar un listado del grupo familiar del paciente.
4	El paciente podrá actualizar sus datos personales de su grupo familiar	El sistema deberá permitir la actualización de los datos personales del grupo familiar del paciente.
5	Visualizar una lista de especialidades médicas disponibles	El sistema proporcionara al paciente información sobre las especialidades médicas.
6	Visualizar una lista de médicos con respecto al especialista	El sistema proporcionara información detallada al paciente sobre los médicos especialistas.
7	Seleccionar a un familiar para la creación de una cita medica	El sistema mostrara un listado para la selección del grupo familiar del paciente
8	Seleccionar fecha y hora para la creación de una cita médica.	El sistema debe permitir la selección de fecha y hora de acuerdo con el horario médico.
9	Visualizar detalle de las citas.	El sistema permitirá información detallada al paciente sobre sus citas médicas registradas.
10	Cancelar cita médica registrada	El sistema permitirá cancelar la cita médica registrada.
11	El paciente podrá dejar una reseña	El sistema deberá permitir el ingreso de un comentario y calificación sobre la atención médica.

12	Generar código de acceso al historial clínico del paciente	El sistema permitirá generar un código de acceso para que el medico tenga acceso al historial clínico del paciente.
13	El medico podrá modificar sus datos	El sistema deberá permitir la modificación de sus datos del médico.
14	Visualizar servicios y precios médicos.	El sistema deberá proporcionar información sobre los servicios, precios de las especialidades médicas.
15	El medico podrá modificar sus servicios y precios	El sistema deberá permitir la modificación de los servicios y precios de las especialidades medicas
16	Visualizar calendario medico	EL sistema deberá proporcionar información sobre los calendarios médicos registrados.
No	**Requerimiento**	**Descripción**
17	El medico podrá agregar nuevos calendarios	El sistema deberá permitir el ingreso de un nuevo calendario donde se seleccionará las fechas, horas disponibles de un médico.
18	Actualizar calendario medico	El sistema permitirá actualizar el calendario medico
19	Visualizar citas registradas de los pacientes.	El sistema deberá proporcionar información al médico sobre las citas programadas por los pacientes
20	Validar código de acceso para ver historial clínico del paciente	El sistema permite validar el código de acceso del paciente para visualizar su historial clínico.
21	Visualizar reseñas registradas por los pacientes	El sistema deberá proporcionar información sobre los comentarios y calificaciones de los pacientes con respecto a la atención médica.
22	Visualizar especialidades medicas	El sistema deberá proporcionar información al administrador sobre las especialidades médicas registradas
23	El administrador podrá registrar especialidades	El sistema deberá permitir el ingreso de nuevas especialidades médicas a la aplicación.

Por otro lado, tenemos los requerimientos no funcionales de la aplicación que se desarrollo

Tabla 12.

Requerimientos no funcionales de la aplicación

N	Requerimientos	Descripción
1	Seguridad	Numero de accesos satisfactorios (NAS) según el rol correspondiente sobre el total de accesos de los usuarios (TAU).
2	Privacidad	El número de usuarios comprometidos (NUC) con su información sobre total de usuarios (TU)

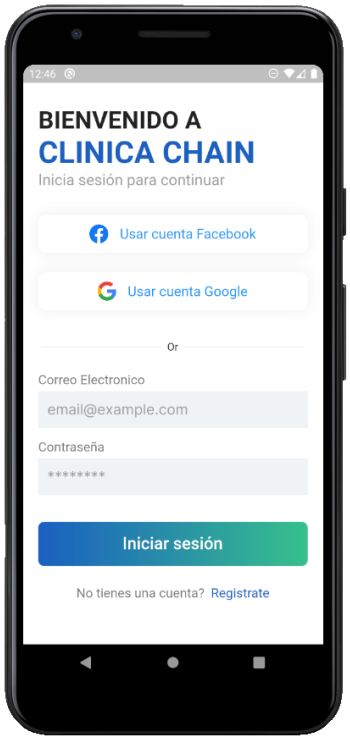
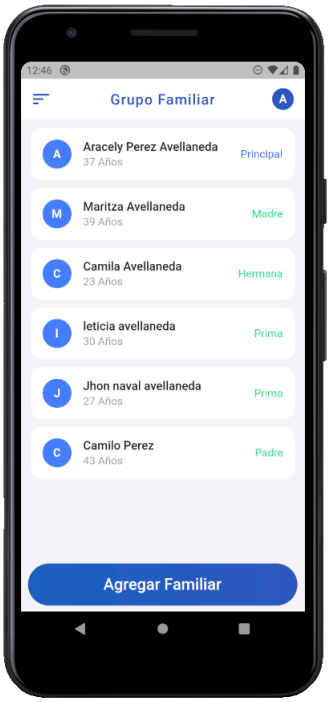


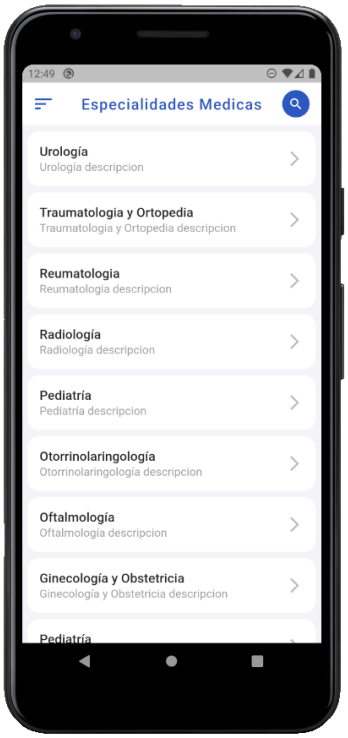
Figura 24. Inicio de sesión de la aplicación para los pacientes, administradores y médicos. Fuente: Elaboración propia.

a.



b.

c.



d.

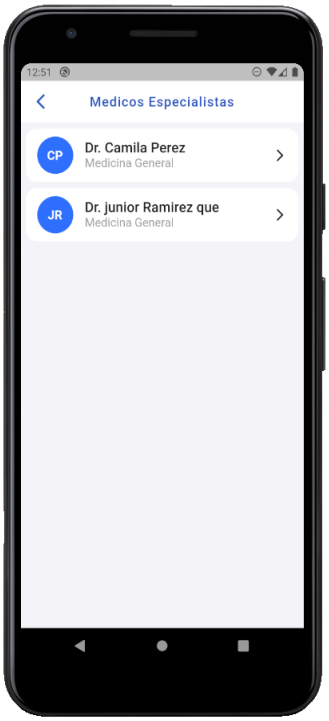
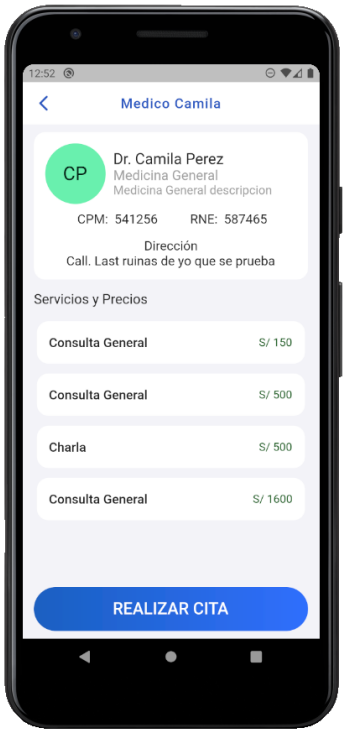
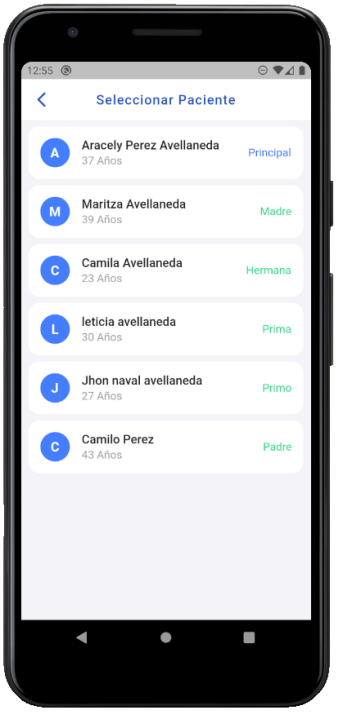


Figura 25. Interfaz de la vista del paciente a. Selección de grupo familiar, b. Formulario de agregar un familiar, c. Selección listas de especialidades, d. Selección médicos. Fuente: Elaboración Propia

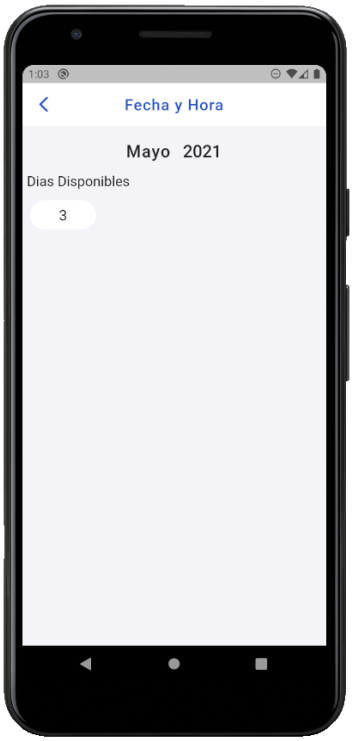
a.



b.



c.



d.

Figura 26. Interfaz de la vista del paciente a. Selección de citas, b. Selección de pacientes, c. Selección de fecha y hora disponible, d. Selección de hora disponible. Fuente: Elaboración Propia

a.

b.

c.

d.

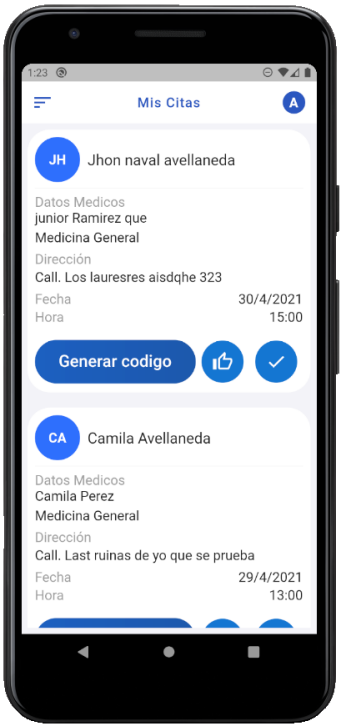
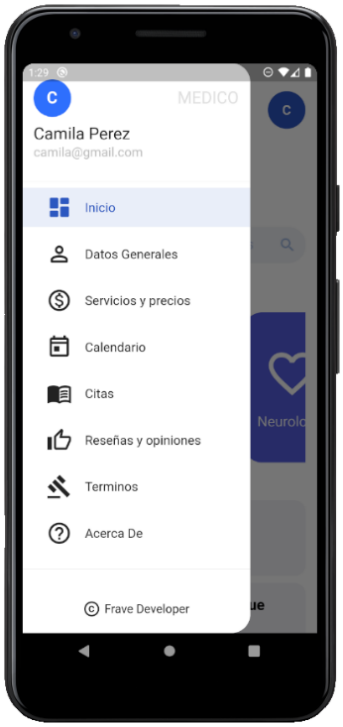
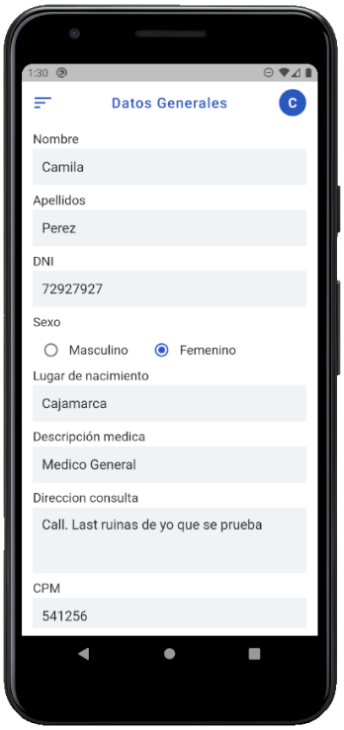


Figura 27. Interfaz de la vista del paciente a. Generar código seguridad, b. Valorar la atención, c. Detalle de la cita, d. Selección de citas. Fuente: Elaboración Propia

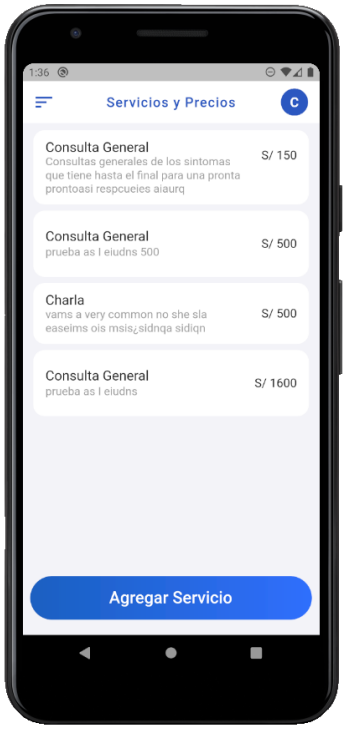
a.



b.



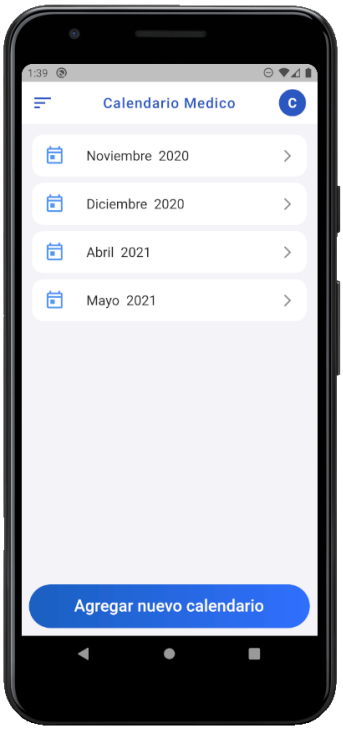
c.



d.

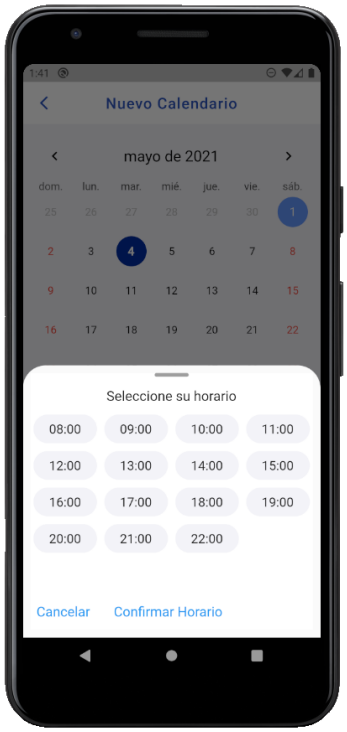
Figura 28. Interfaz de la vista del médico a. Interfaz del médico, b. Datos generales del médico, c. Selección de servicios y precios, d. Ingresar Nuevo servicio médico. Fuente: Elaboración Propia

a.



b.

c.



d.

Figura 29. Interfaz de la vista del médico a. Selección del mes calendario, b. Selección del día, c. Selección de la hora, d. Selección de citas generadas. Fuente: Elaboración Propia

a.

b.

c.

d.

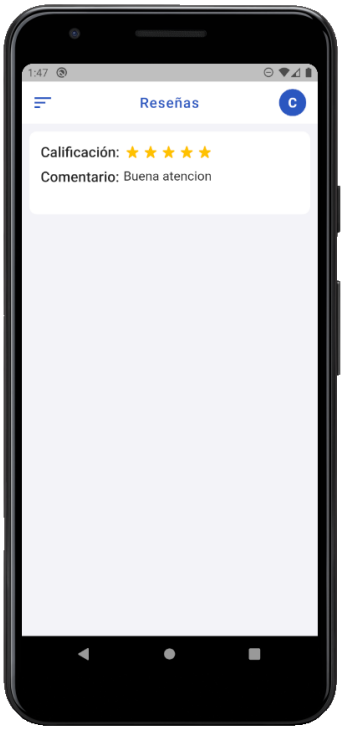
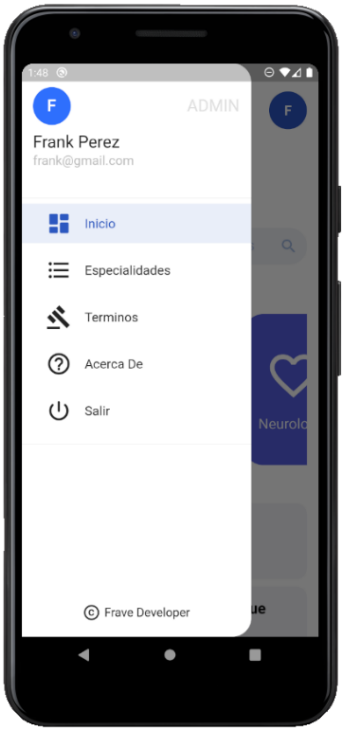
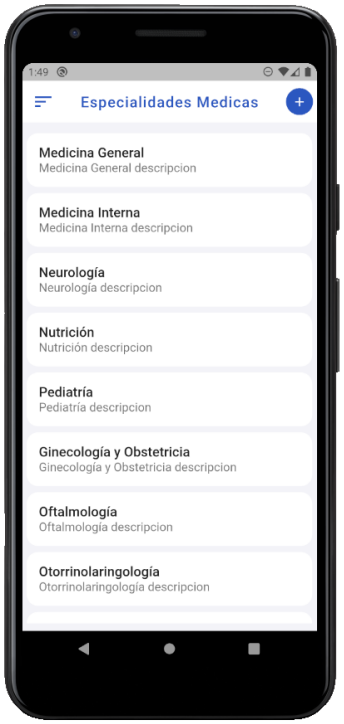


Figura 30. Interfaz de la vista del médico a. Solicitud de código de acceso, b. Listado de Historial Clínico, c. Formulario de la Historia Clínica, d. Reseña del paciente. Fuente: Elaboración Propia

a.



b.



c.

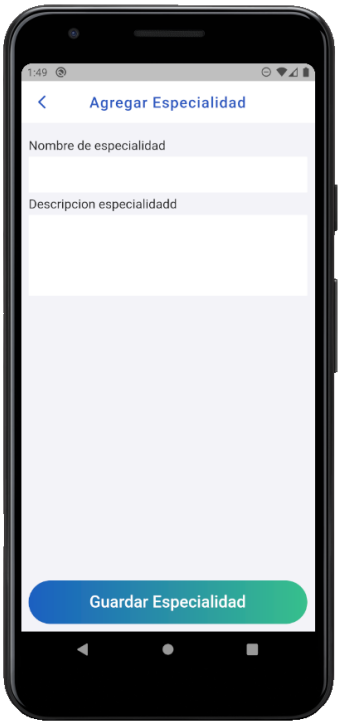


Figura 31. Interfaz de la vista del administrador a. Pantalla principal del administrador, b. Selección de especialistas médicas, c. Formulario para agregar una especialidad Fuente: Elaboración Propia

El proceso de Blockchain inicia cuando el médico, al seleccionar el botón de guardar datos, se ejecuta el código que se muestra en la imagen siguiente:

```
'use strict';

const { Contract } = require('fabric-contract-api');

class ClinicachainContract extends Contract {

    async historiaClinica(ctx, idHistoriaClinica) {
        const buffer = await ctx.stub.getState( idHistoriaClinica );
        return (!!buffer && buffer.length > 0);
    }

    async createHistoriaClinica( ctx, idHistorial, idCita, fecha, pnom
bre, papellido, mnombre, mapellido, mconsulta, ana, pa, pulso, temp, f
c, fr, exmclinico, diagnostico, tratamiento, proximacita ) {
        const exists = await this.historiaClinica( ctx, idHistorial );
        if( exists ){
            throw new Error(`La historia clinica con el Id ${idHistori
al} ya existe`);
        }

        const asset = {
            idHistoriaClinica: idHistorial,
            idCita : idCita,
            fecha_cita : fecha,
            paciente_nombre : pnombre,
            paciente_apellidos : papellido,
            medico_nombre : mnombre,
            medico_apellidos: mapellido,
            motivo_consulta: mconsulta,
            anamnesis: ana,
            pa: pa,
            pulso: pulso,
            temperatura: temp,
            fc: fc,
            fr: fr,
            examen_clinico : exmclinico,
            diagnostico : diagnostico,
            tratamiento: tratamiento,
            proxima_cita : proximacita
        };
```

```
        ctx.stub.putState( idHistorial, Buffer.from( JSON.stringify( asset
 ) ) );
        return JSON.stringify( asset );
    }

    async obtenerHistorialClinico( ctx, idHistoriaClinica ) {
        const exists = await this.clinicachainExists( ctx, idHistoriaClini
ca );
        if( !exists ) {
            throw new Error(`El Paciente ${idHistoriaClinica} no existe`);
        }

        const buffer = await ctx.stub.getState( idHistoriaClinica );
        const asset  = JSON.parse( buffer.toString() );
        return asset;
    }

}

module.exports = ClinicachainContract;
```

Figura 32. Creación del Smart Contract Fuente: Elaboración Propia

La plataforma IBM Blockchain recibe los datos, y se crea el bloque. Una vez creado el bloque se debe ejecutar el código para crear el contrato inteligente.

```
'use strict';

const { FileSystemWallet, Gateway } = require('fabric-network');
const path = require('path');
const fs = require('fs');


exports.registrarHistorial = async function( idHistorial, idCita, fech
a, pnombre, papellido, mnombre, mapellido, mconsulta, ana, pa, pulso,
temp, fc, fr, exmclinico, diagnostico, tratamiento, proximacita ){

    // connect to the connection file
    const ccpPath = path.join(__dirname, './ibpConnection.json');
    const ccpJSON = fs.readFileSync(ccpPath, 'utf8');
    const connectionProfile = JSON.parse(ccpJSON);

    // A wallet stores a collection of identities for use
    const walletPath = path.join(__dirname, './wallet');
    const wallet = new FileSystemWallet(walletPath);
    console.log(`Wallet path: ${walletPath}`);
```

```
    const peerIdentity = 'app-admin';

    try{

        let response;

        // Verificamos si existe un usuario enrolled.
        const userExists = await wallet.exists(peerIdentity);
        if ( !userExists ) {
            response.error = 'Una entidad para el usuario ' + peerIdentity
 + ' no existe en la billeteria. Registre ' + peerIdentity + ' primero';
            return response;
        }

        //Conectando a la red Fabric, pero iniciamos un gateway
        const gateway = new Gateway();

        //usamos la config del archivo, nuestra peerIdentity, y nuestro di
scovery son opciones para conectar a la red de Fabric.
        await gateway.connect(connectionProfile, { wallet, identity: peerI
dentity, discovery: { "enabled": true, "asLocalhost": false } });

        //Conectar a nuestro CANAL que fue creado en IBM Blockchain Plataf
orm
        const network = await gateway.getNetwork('channel1');

        //Nos conectamos a nuestra instancia del contrato que instalamos /
 instancia en IBM Blockchain Plataform
        const contract = await network.getContract('Smart-Contract');

        //Enviamos la transaction a el Contrato inteligente que instalamos
 / instanciamos en el nodo
        response = await contract.submitTransaction('createHistoriaClinica
', idHistorial, idCita, fecha, pnombre,papellido, mnombre, mapellido, mcon
sulta, ana, pa, pulso, temp, fc, fr, exmclinico, diagnostico, tratamiento,
 proximacita );
        response = JSON.parse(response.toString());
        console.log(`respuesta de la transaccion: ${(response)}`)

        console.log('Transaccion enviada con exito!');

        // Nos desconectamos de la red
        await gateway.disconnect();

    }catch( error ){
        console.error(`No se pudo registrar el usuario + ${peerIdentity} +
 : ${error}`);
        let response = {};
        response.error = error;
        return response;
    }
}
```

Figura 33. Creación del bloque Fuente: Elaboración Propia

La realización de las pruebas se obtuvo mediante la elaboración de casos de prueba, teniendo en cuenta el perfil de los usuarios y el entorno del desarrollo, hacia los indicadores de seguridad relacionado al control de acceso y en la privacidad relacionado a la ganancia o pérdida de información.

Para seleccionar el perfil del usuario, solo se ha tenido en cuenta 2 perfiles, el médico cuya característica es que tenga colegiatura habilitada y el paciente cuya característica es que sea mayor de edad.

Tabla 13

Características del perfil del usuario

Características del usuario	Médico	Paciente
Rango Edad	Sin especificar	18 a + años
Genero	Sin especificar	Sin especificar
Discapacidades	Ninguna	Ninguna
Nivel académico	Estudio Superior	Sin especificar

Fuente: Elaboración Propia

Para seleccionar el entorno del test y equipamiento, se consideraron lo siguiente:

Tabla 14

Características entorno de test y equipamiento

Características Entorno	T1
Tipo de Entorno	No controlado
Dispositivo de acceso	Smartphone
Sistema operativo	Android 11
Velocidad de Internet	Estable

Fuente: Elaboración Propia

Se seleccionaron 2 tareas principales en la aplicación para evaluar la funcionalidad del Blockchain según el indicador de privacidad en la medición de la ganancia o pérdida de información propuesto.

Tabla 15

Registrar la Historia Clínica Electrónica en la Base de Datos

Nombre de Tarea	Registrar la Historia Clínica Electrónica en la Base de Datos		
Numero de Tarea	01	**Tipo Usuario:**	Médico
Objetivo Tarea	Agregar la Historia Clínica en la base de datos.		
Secuencia de la tarea o Caso de Prueba	▪ Ingresar a la aplicación ▪ Seleccionar el botón Citas ▪ Seleccionar cita pendiente ▪ Ingresar el código de acceso ▪ Seleccionar nueva Historia Clínica ▪ Llenar los campos de la Historia Clínica ▪ Agregar el nueva Historia Clínica		

Fuente: Elaboración Propia

Tabla 16

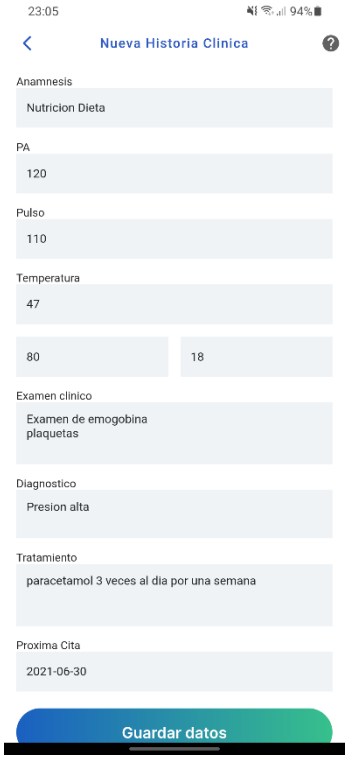
Consultar la última Historia Clínica Electrónica registrada

Nombre de Tarea	Consultar la última Historia Clínica Electrónica registrada		
Numero de Tarea	01	**Tipo Usuario:**	Paciente
Objetivo Tarea	Consultar la última Historia Clínica Electrónica registrada.		
Secuencia de la tarea o Caso de Prueba	▪ Ingresar a la aplicación ▪ Seleccionar el botón Historia Clínica ▪ Seleccionar la última Historia Clínica registrada.		

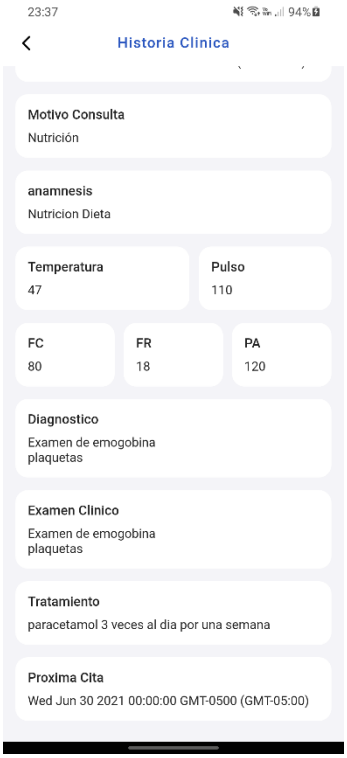
Fuente: Elaboración Propia

Para obtener los datos de este primer indicador se necesitó la participación de 1 médico y 5 pacientes, donde al médico se le asignó realizar 5 veces la tarea de registrar la Historia Clínica en la Base de Datos, y a los pacientes debieron seleccionar su última Historia clínica registrada.

a.



b.



c.

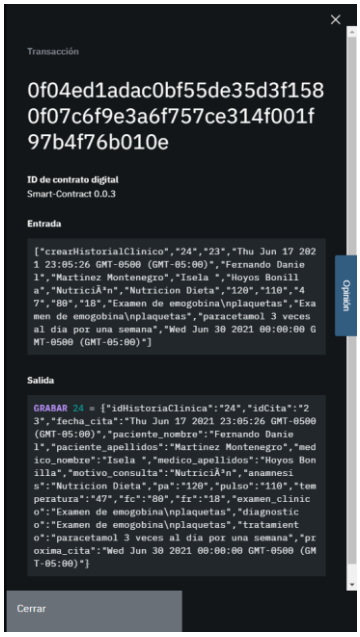


Figura 34. Historia Clínica del paciente a. Formato enviado por el médico, b. Consulta realizada por el paciente, c. Información del bloque en la plataforma IBM
Fuente: Elaboración Propia

Tabla 17

Datos obtenidos de las tareas para el indicador de privacidad.

Tareas/ Usuarios	Tarea 1	Tarea 2	Tareas completadas
Usuario 1	1	1	2
Usuario 2	1	1	2
Usuario 3	1	1	2
Usuario 4	1	1	2
Usuario 5	1	1	2
…			
Usuario 20	1	1	2
			40

Fuente: Elaboración Propia

Para el indicador de seguridad en la medición del control acceso propuesto, se seleccionó una tarea principal en la aplicación para evaluar la funcionalidad del Blockchain.

Tabla 18

Control de acceso para consultar la cadena de bloques

Nombre de Tarea	Consultar la cadena de bloques		
Numero de Tarea	01	**Tipo Usuario:**	Paciente
Objetivo Tarea	Agregar la Historia Clínica en la base de datos.		
Secuencia de la tarea o Caso de Prueba	▪ Ingresar a la aplicación ▪ Seleccionar el botón Historia Clínica ▪ Seleccionar la última Historia Clínica registrada.		

Fuente: Elaboración Propia

Para obtener los datos de este primer indicador se necesitó la participación de 5 pacientes, donde debieron seleccionar su última Historia clínica registrada, y esta debe ser mostrada sin ninguna observación.

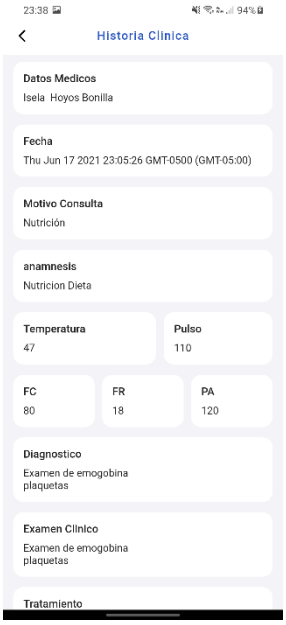


Figura 35. Consulta de una Historia clínica realizada por un paciente Fuente: Elaboración Propia

Tabla 19

Datos obtenidos de las tareas para el indicador de seguridad.

Tareas/ Usuarios	**Tarea 1**	**Tareas completadas**
Paciente 1	1	1
Paciente 2	1	1
Paciente 3	1	1
Paciente 4	1	1
Paciente 5	1	1
…		
Paciente 20	1	1
		20

Fuente: Elaboración Propia

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Como primer objetivo se tuvo, seleccionar la arquitectura blockchain más adecuada para gestión de historias clínicas electrónicas. Con base a la revisión de las literaturas científicas publicadas en diferentes journals, y en los indicadores de privacidad de información y seguridad de los datos de los pacientes. Los resultados indican que la arquitectura Blockchain MA-ABS es la más adecuada para la gestión de historias clínicas electrónicas.

Se realizó una revisión a la arquitectura Blockchain MA-ABS, con el objetivo de caracterizar la cadena de bloques y el proceso del Blockchain, documentándose a través de un esquema y una descripción en el presente informe.

La plataforma tecnológica utilizada es Hyperledger Fabric, en el servicio IBM platform Blockchain, debido a que a diferencia del resto de servicios de plataformas blockchain que existen en el mercado, este brinda una documentación más técnica y un acceso gratuito por un periodo de un tiempo, donde se realizaron las pruebas.

Se desarrolló la aplicación de gestión de historias clínicas, cumpliendo la comunicación con el servicio IBM platform Blockchain.

Con base a los resultados obtenidos en esta investigación, se determinó que la arquitectura Blockchain planteada si cumple con los indicadores de privacidad de información y seguridad de datos. Obteniendo un cien por ciento en las tareas realizadas del control de acceso y privacidad en la información de las historias clínicas de los pacientes, teniendo como resultado cero filtraciones de la información del paciente.

4.2. Recomendaciones

Se recomienda evaluar otras métricas de los indicadores de privacidad de información y seguridad de datos de la arquitectura Blockchain para la obtención de resultados similares.

Se recomienda para obtener mejores resultados crear una red Blockchain con la plataforma tecnológica Hyperledger fabric desde cero, cumpliendo con las características de la arquitectura blockchain.

REFERENCIAS

Abdullah, A. (2018). *Medicalchain*. https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

Alarcon-loayza, L., Rubio-ortiz, C., & Chumán-soto, M. (2019). *Interoperabilidad de Historias Clínicas Electrónicas en el Perú Electronic Health Records interoperability in Peru*. *2*(1), 3–14.

Alexander, J., Smith, J. M., & Smith, J. (2003). Privacy Enhancing Technologies: Third International Workshop, PET 2003, Revised Papers. *Lecture Notes in Computer Science*, *2760*, 88–106. https://doi.org/10.1007/b94512

Alphand, O., Amoretti, M., Claeys, T., Dall ’asta, S., Duda, A., Ferrari, G., Rousseau, F., Tourancheau, B., Veltri, L., Zanichelli, F., & Dall’asta, S. (2018). *IoTChain: A Blockchain Security Architecture for the Internet of Things*. https://hal.archives-ouvertes.fr/hal-01705455

Andersson, C., & Lundin, R. (2008). On the fundamentals of anonymity metrics. *IFIP International Federation for Information Processing*, *262*, 325–341. https://doi.org/10.1007/978-0-387-79026-8_23

Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: Applications in health care. *Circulation: Cardiovascular Quality and Outcomes*, *10*(9), 1–4. https://doi.org/10.1161/CIRCOUTCOMES.117.003800

Arturo de la Torre, Torre, C. de la, & Torre, M. de la. (2017). *Normas ISO 27001-ISO 27002*. 38. www.scprogress.com

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD)*, 25–30. https://doi.org/10.1109/OBD.2016.11

Bambara, J. J., & Allen, P. R. (2018). *Blockchain_ A Practical Guide to Developing Business, Law, and Technology Solutions-McGraw-Hill Education* (M.-H. Education (ed.); Version 1.).

Becerril, H. O. (1999). *EL USO DEL LENGUAJE JAVA COMO UN AMBIENTE DE TRABAJO PARA LA SIMULACIÓN DE ALGORITMOS DISTRIBUIDOS Y DESARROLLO DE SISTEMAS DISTRIBUIDOS*. NSTITUTO TECNOLÓGICO DE ESTUDIOS SUPERIORES DE MONTERREY CAMPUS ESTADO DE MÉXICO.

Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere - A use-case of blockchains in the pharma supply-chain. *Proceedings of the IM 2017 - 2017 IFIP/IEEE International Symposium on Integrated Network and Service Management*, 772–777. https://doi.org/10.23919/INM.2017.7987376

Cachin, C. (2016). Architecture of the Hyperledger Blockchain Fabric. *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL 2016)*, *URL:*, https://www.zurich.ibm.com/dccl/papers/cachin_dccl.

Cearley, D. (2018). *Simposio / ITxpo Gartner 2018*.

Chaum, D. (1988). The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, *1*(1), 65–75. https://doi.org/10.1007/BF00206326

Chen, C., Wang, J., Qiu, F., & Zhao, D. (2016). Resilient Distribution System By Microgrid Formation. *IEEE Transactions on Smart Grid*, *7*(2), 958–966.

Congreso de la República del Perú. (2000). *LEY Nº 27269 | Ley de Firmas y Certificados Digitales*. https://www.minjus.gob.pe/wp-content/uploads/2014/03/Ley27269.pdf

Congreso de la República del Perú. (2011). *Ley N° 29733, Ley de Protección de Datos Personales*. http://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Congreso de la República del Perú. (2013a). *Dictamen 6-2012-2013/CSP-CR*. http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc01_2011.nsf/0/999b23f8c010279105257b2d007a2d57/$FILE/00897DCMAY13032013.pdf

Congreso de la República del Perú. (2013b). *Ley N° 30024 | Ley que crea el Registro Nacional de Historias Clínicas Electrónicas*. https://www.gob.pe/institucion/pcm/normas-legales/240527-30024

Coral, D. L. O. (2018). *REVISIÓN SISTEMÁTICA DEL USO DE BLOCKCHAINS EN DATOS CLÍNICOS Y SU APLICACIÓN EN COLOMBIA* (Issue September). UNIVERSIDAD CATÓLICA DE COLOMBIA.

De Medicina, F., Manuel, J., Belmonte, R., Antonio, D., Badillo, Á., & De La Corte Rodríguez, H. (2016). *UNIVERSIDAD COMPLUTENSE DE MADRID TESIS DOCTORAL Comparación de dos métodos de escritura de historia clínica electrónica MEMORIA PARA OPTAR AL GRADO DE DOCTOR PRESENTADA POR*.

de Oliveira, M. T., Reis, L. H. A., Carrano, R. C., Seixas, F. L., Saade, D. C. M., Albuquerque, C. V, Fernandes, N. C., Olabarriaga, S. D., Medeiros, D. S. V, & Mattos, D. M. F. (2019). Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications. *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 1–6. https://doi.org/10.1109/ICC.2019.8761307

Deshmukh, P. (2017). Design of cloud security in the EHR for Indian healthcare services. *Journal of King Saud University - Computer and Information Sciences*, *29*(3), 281–287. https://doi.org/10.1016/j.jksuci.2016.01.002

Dhariwal, K. (2018). *Blockchain Consensus Mechanisms - Data Driven Investor -*.

Medium. https://medium.com/datadriveninvestor/blockchain-consensus-mechanisms-7aa0176d488a

Diario Norte. (2019). *Historia clínica digital, un salto cualitativo en salud*. http://www.diarionorte.com/article/184514/historia-clinica-digital-un-salto-cualitativo-en-salud

Díaz, C., Seys, S., Claessens, J., & Preneel, B. (2003). *Towards measuring anonymity*. http://www.esat.kuleuven.ac.be/cosic/

Dios, T. J. R. de, Bordonabe, B. L., Ochoa, G. L., & Fernández, J. L. S. (2017). *Grupo Auxiliar de la Función Administrativa. Servicio de Salud de Castilla-La Mancha (SESCAM). Temario y Test.* (ERadio (ed.); Volumen 2). https://books.google.com.pe/books?id=8DorDgAAQBAJ&pg=PA656&lpg=PA656&dq=es+el+conjunto+de+medidas+preventivas+y+reactivas+de+las+organizaciones+y+de+los+sistemas+tecnológicos+que+permiten+resguardar+y+proteger+la+información+buscando+mantener+la+confidenc

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and Trustable Electronic Medical Records Sharing using Blockchain. *AMIA ... Annual Symposium Proceedings. AMIA Symposium*, *2017*, 650–659.

Ethereum. (2019). *Ethereum*. https://www.ethereum.org/

Eyal, I., & Sirer, E. G. (2018). Majority is not Enough: Bitcoin Mining is Vulnerable. *NSF Trust STC and by DARPA*.

Gaur, N., Desrosiers, L., Novotny, P., Ramakrishna, V., O'Dowd, A., & Baset, S. (2018). *Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer*. Packt Publishing.

Gervais, A. (2016). *On the Security and Performance of Proof of Work Blockchains Vasileios Glykantzis Srdjaň Capkun*. https://bitcoin.org/en/developer-reference#data-messages

Gestion Medica. (2015). *Mejor Software Medico. Análisis comparativo los software para clinicas Historia Clínica en la Nube, ¿es más segura?* https://gestionmedica.org/historia-clinica-en-la-nube/

Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems. *IEEE Access*, *6*, 11676–11686. https://doi.org/10.1109/ACCESS.2018.2801266

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2006). *Metodología de la investigación.* (M.-H. / INTERAMERICANA (ed.)).

Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers and Security*, *53*, 1–17. https://doi.org/10.1016/j.cose.2015.05.002

HIPAA JOURNAL. (2019). *July 2019 Healthcare Data Breach Report*. https://www.hipaajournal.com/july-2019-healthcare-data-breach-report/

Hontoria, A. (2018). *Blockchain, ejemplo de intercambio de información - The Black Box Lab*. https://theblackboxlab.com/2018/10/25/ejemplo-practico-blockchain/

Hurtado, I. F. (2018). *Hyperledger Fabric — En 4 minutos - Inteligencia Logística -*. Medium. https://medium.com/inteligencia-logística/hyperledger-fabric-resumen-y-conclusión-bc43213a86d8

Hyperledger. (2019). *Hyperledger*. https://www.hyperledger.org/%0D

IBM. (2022). *IBM Blockchain Platform for IBM Cloud*. https://cloud.ibm.com/docs/blockchain

Interoperabilidad e intercambio de información de salud | HIMSS. (n.d.). Retrieved October 15, 2019, from https://www.himss.org/library/interoperability-health-information-exchange

ISO/IEC. (2013). *ISO 27002:2013*.

Jothi, N., Rashid, N. A., & Husain, W. (2015). Data Mining in Healthcare - A Review. *Procedia Computer Science*, *72*, 306–313. https://doi.org/10.1016/j.procs.2015.12.145

Kelly, D. J., Baldwin, R. O., Raines, R. A., Grimaila, M. R., & Mullins, B. E. (2008). A survey of state-of-the-art in anonymity metrics. *Proceedings of the ACM Conference on Computer and Communications Security*, 31–39. https://doi.org/10.1145/1456441.1456453

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Applied Sciences*, *9*(9), 1736. https://doi.org/10.3390/app9091736

Kuo, T.-T., Hsu, C.-N., & Ohno-Machado, L. (1385). *ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks*. http://www.ghbook.ir/index.php?name=های رسانه و فرهنگ نوین&option=com_dbook&task=readonline&book_id=13650&page=73&chkhashk=ED9C9491B4&Itemid=218&lang=fa&tmpl=component

Laurence, T. (2017). *Blockchain For Dummies* (I. John Wiley & Sons (Ed.)).

Levy, H. P. (2018). *The Reality of Blockchain - Smarter With Gartner*. https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/

Li, J., Au, M. H., Susilo, W., Xie, D., & Ren, K. (2010). Attribute-based signature and its applications. *Proceedings of the 5th International Symposium on Information, Computer and Communications Security, ASIACCS 2010*, 60–69. https://doi.org/10.1145/1755688.1755697

Li, Y.-C. J., Yen, J.-C., Chiu, W.-T., Jian, W.-S., Syed-Abdul, S., & Hsu, M.-H. (2015). Building a national electronic medical record exchange system - experiences in Taiwan. *Computer Methods and Programs in Biomedicine*, *121*(1), 14–20. https://doi.org/10.1016/j.cmpb.2015.04.013

Marc, P. (2016). *Blockchain Technology: Principles and Applications*.

MedChain. (2019). *MedChain And The Future Of EMR Interoperability*. https://www.medchain.us/

Medium. (2019). *¿Quieres desarrollar en blockchain?* https://medium.com/@1o1marketing.cs2/quieres-desarrollar-en-blockchain-4015c7f573d5

MINJUS. (2013). *Resolución Directoral de aprobación de la directiva de seguridad de la información administrada por los Bancos de Datos Personales*. https://www.minjus.gob.pe/wp-content/uploads/2013/10/RD-Directiva-de-Seguridad.pdf

MINSA. (2011). *Resolución Ministerial N° 576-2011-MINSA*. https://www.gob.pe/institucion/minsa/normas-legales/243313-576-2011-minsa

MINSA. (2016). *Resolución Ministerial N° 978-2016-MINSA*. https://www.gob.pe/institucion/minsa/normas-legales/191446-978-2016-minsa

MINSA. (2018). *Resolución Ministerial N° 214-2018-MINSA*. Diario El Peruano. https://www.gob.pe/institucion/minsa/normas-legales/187487-214-2018-minsa

Resolución_Ministerial_N__618-2019-MINSA, (2019). https://cdn.www.gob.pe/uploads/document/file/340420/Resolución_Ministerial_N__618-2019-MINSA.PDF

Morkunas, V. J., Paschen, J., & Boon, E. (2019). How blockchain technologies impact your business model. *Business Horizons*, *62*(3), 295–306. https://doi.org/https://doi.org/10.1016/j.bushor.2019.01.009

Murdoch, S. J. (2014). Quantifying and measuring anonymity. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8247 LNCS*, 3–13. https://doi.org/10.1007/978-3-642-54568-9_1

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Nam, C. (2006). *ASSOCIATION FOR CONSUMER RESEARCH Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online*. http://www.acrwebsite.org/volumes/12442/volumes/v33/NA-33http://www.copyright.com/.

Olavarría. (2019). *El sistema "Historia Clínica Electrónica."* InfoSeptima.

http://infoseptima.com.ar/presentaron-el-sistema-historia-clinica-electronica/

Omar, A. Al, Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems*, *95*, 511–521. https://doi.org/10.1016/j.future.2018.12.044

Panetta, K. (2018). *Gartner Top 10 Strategic Technology Trends for 2019 - Smarter With Gartner*. https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/

Purkayastha, S. (2019). *Eight Blockchain platforms for rapid prototyping – RadioStudio*. https://radiostud.io/eight-blockchain-platforms-comparison/

RAE. (n.d.). *Definición de interoperabilidad*. Retrieved October 15, 2019, from https://dej.rae.es/lema/interoperabilidad

Rodriguez, N. (2018). *La Web 3.0 estará impulsada por la tecnología Blockchain Stack*. https://101blockchains.com/es/web-3-0-tecnologia-blockchain-stack/#prettyPhoto/0/

Rojas, D., Alburquerque, J., Bermejo, J., Blanco, Ó., Carnicero, J., Escolar, F., Fernández, A., García, M., Hualde, R. S., Huneeus, D., Lagarto, J., Teresa Martínez-Berganza, M., Mazón, A. L., Oviedo, E., & Quintana, F. (2011). *Manual de salud electrónica para directivos de servicios y sistemas de salud*.

Schneider Zurich, M. (2017). *Design and Prototypical Implementation of a Blockchain-based System for the Agriculture Sector*. http://www.csg.uzh.ch/

Shuaib, Saleous, Shuaib, & Zaki. (2019). Blockchains for Secure Digitized Medicine. *Journal of Personalized Medicine*, *9*(3), 35. https://doi.org/10.3390/jpm9030035

The Economist. (2015). *The great chain of being sure about things*.

Wagner, I., & Eckhoff, D. (2018). Technical privacy metrics: A systematic survey. *ACM Computing Surveys*, *51*(3). https://doi.org/10.1145/3168389

Wood, G. (2017). Ethereum: A Secure Decentralised Generalised Transaction Ledger. EIP-150 REVISION (030c1b5 - 2017-07-10). *2017*, *August 1*, *2017*, 33.

Xie, Z., Dai, S., Chen, H.-N., & Wang, X. (2018). Blockchain challenges and opportunities: a survey. In *International Congress on Big Data* (Vol. 14, Issue 4).

Yang, Y., Lutes, J., Li, F., Luo, B., & Liu, P. (2012). *Stalking Online: on User Privacy in Social Networks*.

Yuan, Y., & Wang, F.-Y. (2018). Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Transactions on Systems, Man, and*

Cybernetics: Systems, *48*(9), 1421–1428. https://doi.org/10.1109/TSMC.2018.2854904

Zeadally, S., Pathan, A. S. K., Alcaraz, C., & Badra, M. (2013). Towards privacy protection in smart grid. *Wireless Personal Communications*, *73*(1), 23–50. https://doi.org/10.1007/s11277-012-0939-1

ANEXOS

Resolución de aprobación de proyecto

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0451-2021/FIAU-USS

Pimentel, 28 de mayo de 2021

VISTO:
El Acta de reunión N°1305-2021 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida mediante oficio N°0227-2021/FIAU-IS-USS de fecha 19 de mayo de 2021, y;

CONSIDERANDO:
Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y tesis son aprobados por el Comité de Investigación y derivados a la Facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El periodo de vigencia de los mismos será de dos años, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; es individual o en pares para obtener un título profesional. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, según documentos de Vistos el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acuerdan aprobar los temas de las Tesis a cargo de los estudiantes del curso de Investigación II que se detallan en el anexo de la presente Resolución.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1°: APROBAR, el tema de la Tesis perteneciente a la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de los estudiantes del Programa de estudios de INGENIERÍA DE SISTEMAS según se detalla en el anexo de la presente Resolución.

ARTÍCULO 2°: ESTABLECER, que la inscripción del Tema de la Tesis se realice a partir de emitida la presente resolución y tendrá una vigencia de dos (02) años.

ARTÍCULO 3°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Dr. [illegible] Ramos Monzel
Decano - Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC

MBA. María Rosita Suárez Rivera
Secretaria Académica / Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC

Cc: Interesado, Archivo

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0451-2021/FIAU-USS

Pimentel, 28 de mayo de 2021

ANEXO

N°	AUTOR (ES)	TEMA DE TESIS
1	BECERRA SANCHEZ MIGUEL ANGEL	EVALUCION DE RENDIMIENTO DE PROTOCOLOS DE COMUNICACIÓN DE IOT EN EL MONITOREO DE LA CALIDAD DEL AIRE
2	BOCANEGRA PINCHI YAN CARLOS	DESARROLLO DE UNA METODOLOGÍA PARA LA ADQUISICIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN ORIENTADA A PEQUEÑAS ORGANIZACIONES BASADA EN ESTÁNDARES
3	BRENIS LLAGUENTO JULIO ANTONIO	COMPARACIÓN DE PROTOCOLOS DE AUTENTICACIÓN EN CONEXIONES DE REDES PRIVADAS VIRTUALES PARA USO EN TRABAJO REMOTO. CASO DE ESTUDIO: MUNICIPALIDAD PROVINCIAL DE FERREÑAFE
4	- CARREÑO CASTILLO JORGE LUIS - SALAZAR AGUILAR LUIS	EVALUACIÓN DE ALGORITMOS PARA MEDIR EFICIENCIA EN EL TRAFICO OCULTO DE VOZ IP
5	CARREÑO GUERRERO SANTIAGO ANIBAL	MODELO PREDICTIVO DEL PROCESO DE VENTAS UTILIZANDO INTELIGENCIA DE NEGOCIOS Y DATA ANALITICS EN LA EMPRESA CENTRO TEXTIL DE LA MATTA S.A.C.
6	CARRERA SANCHEZ JOSE ANTONIO	EVALUACIÓN DE MARCOS DE TRABAJO PHP PARA EL DESARROLLO DE APLICACIONES WEB, BAJO LA NORMA ISO/IEC 25010, ENFOCADA A LA CALIDAD EN USO DEL PRODUCTO
7	CASTILLO CARDENAS JOSE LEONARDO	ANÁLISIS COMPARATIVO DE TÉCNICAS DE EVALUACIÓN EN USABILIDAD PARA MEDIR CALIDAD EN USO DE APLICACIONES WEB EN PEQUEÑAS EMPRESAS
8	CHIMPEN SERQUÉN MERLINA JESSICA	DISEÑO DE UNA MESA DE AYUDA BASADO EN BPMN E ITIL V3 PARA EL AREA DE TI DE LA MUNICIPALIDAD PROVINCIAL DE LAMBAYEQUE
9	CORONEL CAJAN ERICK ARTURO	RECONOCIMIENTO DE EXPRESIONES FACIALES DE TRISTEZA UTILIZANDO APRENDIZAJE PROFUNDO
10	- CORTEZ BURGOS JOHANDER ENRIQUE - MEDRANO MORI JOSE LUIS	DESARROLLO DE UN MODELO DE PROCESOS PARA UNA FÁBRICA PERUANA DE SOFTWARE BASADA EN METODOLOGÍAS ÁGILES CASO DE ESTUDIO CONASTEC S.R.L.
11	CRUZADO PEREZ SANDRA MARIANA	EVALUACIÓN DE EFECTIVIDAD DE UNA METODOLOGÍA ÁGIL DE ARQUITECTURA EMPRESARIAL PARA ALINEAR LOS SERVICIOS DE TI CON LOS OBJETIVOS DEL NEGOCIO EN UNA MICRO EMPRESA PERUANA DEL RUBRO DE MARKETING
12	FLORES ALEJANDRIA RONY ASUNCION	MODELO DE CALIDAD BASADO EN ESTANDARES PARA LOS PROCESOS DE DESARROLLO DE SOFTWARE EN PEQUEÑAS ORGANIZACIONES. Caso de estudio: Soluciones Virtuales VAIXS
13	- HUAMAN CASAS JUNIOR ALDAIR - SERRATO VILCHERRES FERNANDO JOSE	DESARROLLO DE UN MÉTODO PARA DETECCIÓN DE FRAUDES DE PAGOS EN LÍNEA UTILIZANDO APRENDIZAJE AUTOMÁTICO
14	MARTINEZ MONTENEGRO FERNANDO DANIEL	EVALUACIÓN DE ARQUITECTURA BLOCKCHAIN MA-ABS PARA LA GESTIÓN DE HISTORIAS CLÍNICAS ELECTRÓNICAS PERUANAS
15	PEREZ AVELLANEDA FRANKLIN	EVALUACIÓN DE ARQUITECTURA BLOCKCHAIN BASADO EN GUANG YANG PARA LA GESTIÓN DE HISTORIAS CLINICAS ELECTRONICAS PERUANAS
16	MENDOZA RENGIFO GENARO	DESARROLLO DE UNA METODOLOGÍA ÁGIL AD HOC PARA LA CREACIÓN DE APLICACIONES WEB EN PEQUEÑAS EMPRESAS. CASO DE ESTUDIO: SOLTI S.A.C
17	- MONTALVO SANDOVAL JOSE LUIS - RUBIO OTERO DANIEL	DESARROLLO DE UN MÉTODO DE IDENTIFICACIÓN DE DEFECTOS EXTERNOS DEL MANGIFERA INDICA L USANDO PROCESAMIENTO DE IMÁGENES DIGITALES Y APRENDIZAJE DE MÁQUINA
18	OLIVOS JULCA CHARLES	COMPARACIÓN DE TÉCNICAS DE RECONOCIMIENTO FACIAL PARA CONTROLAR LA ASISTENCIA DE LOS

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0451-2021/FIAU-USS

Pimentel, 28 de mayo de 2021

N°	AUTOR (ES)	TEMA DE TESIS
		ESTUDIANTES DE NIVEL SECUNDARIO DE UNA INSTITUCIÓN EDUCATIVA
19	ORTEGA PUENTE OSCAR FERNANDO	DESARROLLO DE UNA APLICACIÓN MÓVIL DE REPORTE CIUDADANO UTILIZANDO IMÁGENES Y GEOLOCALIZACIÓN
20	PISFIL JAUREGUI JOSE LAURENT	SISTEMA WEB BASADO EN MICROSERVICIOS PARA MEJORAR LA INTEROPERABILIDAD DEL PROCESO DE CONSULTAS DE ARBITRIOS TRIBUTARIOS EN MUNICIPALIDADES
21	RAVELO RUIZ ALLEN MARCEL	EVALUACIÓN DE ALGORITMOS DE PREDICCIÓN APLICADOS AL MANTENIMIENTO PREDICTIVO DE MÁQUINAS ELÉCTRICAS ROTATIVAS
22	SUCLUPE CHAPOÑAN MANUELA DEL ROSARIO	SISTEMA DE INFORMACIÓN LOGÍSTICA PARA MEJORAR LA GESTIÓN Y CONTROL DEL PROCESO DE ALMACENAMIENTO DE LA CONSTRUCTORA YAVARI S.R.L. - PROVINCIA DE MAYNAS-LORETO.
23	VILLEGAS CASTAÑEDA CESAR RUDECINDO	ANÁLISIS COMPARATIVO DE SISTEMAS GESTORES DE BASE DE DATOS RELACIONAL Y NO RELACIONAL EN EL CONTEXTO DEL MANEJO DE INFORMACIÓN DE GRUPOS DE RESCATE INTERNACIONAL EN DESASTRES

Consentimiento informado

ANEXO 03: Instrumentos de recolección de datos

Tabla 20

Formato del instrumento de recolección de datos

Nombre de Tarea	(Se detalla el nombre de la Tarea)		
Numero de Tarea	(N° Tarea)	**Tipo Usuario:**	(Tipo Usuario)
Objetivo Tarea	(Objetivos de la Tarea)		
Secuencia de la tarea o Caso de Prueba	(Secuencia de la Tarea)		

Tabla 21

Instrumento Ficha de observación

Tareas/ Usuarios	**Tarea 1**	**Tareas completadas**
Paciente 1	1	1
Paciente 2	1	1
Paciente 3	1	1
Paciente 4	1	1
Paciente 5	1	1
		5

Tabla 22

Anexo 04 Ventajas y Desventajas arquitecturas Blockchain

Proyecto arquitectura blockchain	Año	Ventajas	Desventajas
MedRec	2016	Primer proyecto implementado Aborda problemas de fragmentación, accesibilidad lenta, interoperabilidad del sistema y agencias de pacientes. Cifrado y pistas de auditoría Satisfacción de HIPAA	Los datos deben ser extraídos Problemas de seguridad de punto final Problemas de escalabilidad
Healthcare Data Gateways	2016	Anonimización de datos Simplifica datos singulares del paciente	Administrar diferentes tipos de datos Mantener los datos privados mientras se ejecutan los cálculos.
Stony Brook Study	2017	El paciente tiene control de acceso. Los datos están encriptados Los datos se almacenan en la nube. Asegura la disponibilidad del servicio Satisfacción de HIPAA	Los datos no están categorizados Problemas de interoperabilidad con otros sistemas y tipos de datos
Patientory	2017	Gestión en tiempo real Almacenamiento seguro Control de acceso	Pagar por almacenamiento Incentivos a los mineros Uso de tokens
Modum.io AG	2017	Caso de uso con gestión farmacéutica Capacidad para trabajar sin conexión Recopila y rastrea datos de dispositivos IoT Preserva la integridad de los datos.	Bifurcar Ethereum puede causar fallas Vulnerabilidad DoS Problemas de escalabilidad
TMSMD	2017	Cifrado de datos y servidor Compartir registros de pacientes Control de acceso	Sin cumplimiento de la normativa de privacidad
MeDShare	2017	Los datos se almacenan en la nube. Anonimato de los datos	
MedRec 2.0	2018	Contratos inteligentes para vincular direcciones a datos Seudónimo No hay un solo punto de ataque Aborda la vulnerabilidad del contrato inteligente Restringe el almacenamiento de blockchain a las identidades Satisfacción de HIPAA	Problemas de seguridad de punto final Escalabilidad Inferencia del paciente
MedicalChain	2018	Permite la comunicación entre diferentes médicos. Doble encriptación para mayor privacidad y seguridad. Centrado en el paciente	Requiere cryptofuel / moneda Posibilidad de no adquirir fichas al comprarlas No hay control sobre los tokens
Smart Contracts for Wearables	2018	Los datos se almacenan en la nube. Mayoría de firmas necesarias para la validación de bloque Control de acceso Satisfacción de HIPAA	Comunicación por canal abierto Tiempo de transmisión de datos Los nodos deben permanecer en línea para el consenso
Identity and Access Management	2018	Acceso y control de identidad Registro para usuarios Las entidades están aprobadas por el paciente.	Problemas de escalabilidad
PBE-DA	2018	Dispositivos IoT liberados de la generación y autenticación de claves. Seudónimo	Blockchain no totalmente integrado No se menciona el cumplimiento de la normativa de privacidad. Vulnerable al ataque
Clinical Trials Monitoring	2018	Cifrado Control de acceso Monitoreo en tiempo real	Se requieren permisos para acceder a las bases de datos clínicas Problemas de interoperabilidad entre diferentes clínicas y partes
Blockchain-based Digital Health Information Exchange	2018	Privacidad de datos Aborda preocupaciones de política y acceso a datos Castigos de violación	Escalabilidad Tamaño de datos
MA-ABS	2018	Seguridad de datos Preservar la privacidad Anonimato y la inmutabilidad de la información	Costo de este protocolo aumenta al número de autoridades
Ancile	2018	Seguridad e Interoperabilidad	Incentivos a los mineros
MediBChain	2019	Solo las partes registradas pueden participar Seudónimo No se puede acceder a los datos sin procesar de otras partes Autenticación con actividad	Los contratos inteligentes requieren cryptofuel No hay robo clave / recuperación de pérdidas Sin interoperabilidad

Tabla 23

Anexo 05 Arquitecturas mejor evaluadas

Proyecto arquitectura blockchain	Año	Ventajas	Desventajas
MA-ABS	2018	Seguridad de datos Preservar la privacidad Anonimato y la inmutabilidad de la información	Costo de este protocolo aumenta al número de autoridades
Ancile	2018	Seguridad e Interoperabilidad	Incentivos a los mineros
Identity and Access Management	2018	Acceso y control de identidad Registro para usuarios Las entidades están aprobadas por el paciente.	Problemas de escalabilidad