BLOCKCHAIN

Prototipo orientado a las historias clínicas

UNIVERSIDAD DE PAMPLONA- ALEJANDRO VARELAS

Desarrollo de un prototipo de una plataforma de registro de historias clínicas basado en Tecnología Blockchain Hospital San Juan De Dios de Pamplona

autor

EDUAR ALEJANDRO VARELAS ARROYAVE

INGENIERA TELECOMUNICACIONES

DEPARTAMENTO INGENIERIA ELECTRICA, ELECTRONICA, SISTEMAS Y TELECOMUNICACIONES

INGENIERÍAS Y ARQUITECTURA

UNIVERSIDAD DE PAMPLONA

PAMPLONA 2020

Desarrollo de un prototipo de una plataforma de registro de historias clínicas basado en Tecnología Blockchain Hospital San Juan De Dios de Pamplona

autor

EDUAR ALEJANDRO VARELAS ARROYAVE

Director

YESID ALEXANDER MADRID CARRILLO

INGENIERO DE SISTEMAS - FÍSICO

INGENIERA TELECOMUNICACIONES

DEPARTAMENTO INGENIERIA ELECTRICA, ELECTRONICA, SISTEMAS Y TELECOMUNICACIONES

INGENIERÍAS Y ARQUITECTURA

UNIVERSIDAD DE PAMPLONA

PAMPLONA 2020

Dedicatoria

Dedicatoria especial a quienes se han esmerado por brindarme la oportunidad de formarme como profesional, mi familia encabezada por mi mama y mi abuela, gracias a su apoyo incondicional hoy puedo comprender el esfuerzo y ver reflejado los años de dedicación.

Agradecimientos

¡A DIOS PRIMERAMENTE!
Agradecimiento especial a quienes hicieron parte de tan esmerado y luchado sueño, completar mi programa universitario en el que siempre conté con el apoyo de docentes, directores y compañeros, muchos de ellos reflejaron sus buenas costumbres y modales, en el ámbito personal y en el ámbito profesional fueron guías admirables en su labor de instructores, inculcando siempre el deseo de prevalecer, mantener y poner a filo todos los conocimientos, se mostraron como proyecciones para el desarrollar del saber y la investigación . Generalmente agradecer a la Universidad de Pamplona por la ardua y especial labor de formar líderes integrales y significativos para la sociedad.

Agradezco a quienes fueron elegidos como jurado de mi proyecto de grado por sus buenos deseos y orientación hacia la excelencia de mi trabajo. Nidia Sandoval y Marleny Fernández docentes que se reconocen por su intachable desempeño y gran conocimiento en las áreas de la ingeniería, un cálido abrazo por su entendimiento y enseñanzas durante semestres de arduo trabajo y desempeño.

Al ingeniero Yesid Madrid quien aceptó ser mi director de grado en una condición tan precaria como lo es la pandemia 2020, poniéndose en total disposición en lo que contextualiza un tutor de grado, un gran agradecimiento especial y éxitos en la evolución de sus carreras.

Al director del programa, Ingeniero Hernando Velandia mi total admiración y agradecimiento por sus cualidades profesionales y personales, siempre estuvo presto para atender a todas las solicitudes y peticiones. Además, un agradecimiento a los profesores del programa que durante los últimos semestres siempre brindaron sus cualidades personales y profesionales, contando con su excelencia y dedicación. Jhorman Vides, Mauricio Sequeda, German Portilla, Jose Del Carmen Santiago…

Por último y no menos importante, agradezco a mi madre quien hizo de este sueño una realidad con su entrega, paciencia y apoyo incondicional.

Abstract

Blockchain is a technology of a distributed and incorruptible typology, since there is no hierarchical scheme that allows the alteration of any character in the source file, its use could change the management in the health sector allowing the immutability of the data, sharing them once they are you are certain of the validation and its security. In this document, a prototype of clinical data transactions through distributed network technology is developed, the traceability of the data allows knowing what has happened at all times within the chain by any of the agents, giving access to the data at any time or place, using any network device, in the public health sector Hospital San Juan De Dios will help manage health systems in a more efficient way, also making processes shorter, favoring prevention models. The results can be evaluated once the prototype is running locally on a computer with Windows 7 operating system, developing a programming code in Python language for its characteristics mentioned in the client server execution model in the document, it is evidenced as the multiple Advantages of deploying processes of distributed network typologies can be efficient in order to put the patient in full control of their clinical data so that they have an instant and secure legitimacy of their processes through transactions on the blockchain , proving to be an innovative solution to the way of transferring clinical data with a security layer, the final prototype must have the validity requirements to deploy a chain of blocks, safe and verifiable results that will be visible in the results chapter of the document. This prototype could turn out to be a way out of the centralized networks, in the health sector it becomes an imminent need for the control of clinical data, at a general level it points to a global health ecosystem, seeking accessibility anywhere in the world..

Tabla de Contenidos

Lista de figuras

Lista de cuadros

Introducción

1.1 Resumen

Blockchain es una tecnología de tipología distribuida e incorruptible, ya que no existe esquema jerárquico que permita la alteración de ningún carácter del archivo fuente, su uso podría cambiar la gestión en el sector de la salud permitiendo la inmutabilidad de los datos, compartiéndolos una vez se tiene certeza de la validación y su seguridad. En este documento se desarrolla un prototipo de transacciones de datos clínicos a través de tecnología de red distribuida, la trazabilidad del dato permite saber qué ha ocurrido en todo momento dentro de la cadena por cualquiera de los agentes, dando acceso a los datos en cualquier momento o lugar, usando cualquier dispositivo de red, en el sector de salud pública Hospital San Juan De Dios ayudará a gestionar los sistemas de salud de una forma más eficiente, además logrando que los procesos sean más cortos favoreciendo los modelos de prevención. Los resultados se podrán evaluar una vez el prototipo esté corriendo de manera local en una computadora con sistema operativo Windows 7, desarrollando un código de programación en lenguaje Python por sus características mencionadas en el modelo de ejecución cliente servidor en el documento se evidencia como las múltiples ventajas de desplegar procesos de tipologías de red distribuidas pueden ser eficientes con el objetivo de poner al paciente en control total de sus datos clínicos para que este tenga una legitimidad de sus procesos de manera instantánea y segura a través de las transacciones en la cadena de bloques, resultando ser una innovadora solución a la forma de transferir datos clínicos con una capa de seguridad, el prototipo final deberá tener los requisitos de validez para desplegar una cadena de bloques, segura y verificable resultados que serán visibles en el capítulo de resultados del documento. Dicho prototipo podría resultar siendo un camino de salida de las redes centralizadas, en el sector salud se convierte en una necesidad inminente para el control de los datos clínicos, a nivel general apunta a un ecosistema sanitario mundial, buscando la accesibilidad en cualquier lugar del mundo.

1.2 Planteamiento de problema

Los datos médicos que pertenecen a cada paciente de la nación están en control de entidades que tercerizan la información. Por lo tanto, limitan el manejo y la privacidad de los mismos; esto ocasiona múltiples consecuencias con las que día a día los usuarios se sienten más inconformes, pues la necesidad de controlar de manera segura y eficiente cada proceso en su historia de salud se convierte en una necesidad inminente, además de las adversidades que tienen los documentos ubicados en un sitio físico, en el control y manejo de carpetas, la migración de estos procedimientos de datos a la digitalización abre otros retos en el mundo de la ingeniería. Ahora los inconvenientes vienen dentro de los sistemas de cómputo encargados de procesar la data digital dando lugar a la ciberseguridad, siendo esta la práctica de defender los computadores, servidores, sistemas electrónicos y redes de ataques maliciosos poniendo la era digital en desarrollo evolutivo alcanzando lo que podría ser la solución (BLOCKCHAIN).

¿podría un prototipo de historias clínicas basado en tecnología distribuida "blockchain" solucionar este y otro problemas que arraiga la información médica a través de sistemas de softwares? La medicina apunta a un ecosistema sanitario mundial con el mayor número de beneficios y consideraciones para los usuarios que participaran en ella, la tecnología blockchain sin duda alguna comprende y brinda beneficios en lo que se refiere a estabilidad y seguridad de la información.

1.3 Justificación

La red de datos basada en blockchain es una solución viable para el complejo problema de compartir datos de salud a través de sistemas informáticos, siendo uno de los conceptos que más relevancia tiene en el mundo de la criptografía digital. La tokenización es un concepto que se refiere a la transformación y representación de un activo u objeto real como una expresión de datos únicos dentro de la blockchain, permitiendo una representación única e inmutable que dará como resultado un "objeto digital" que contiene la descripción de dichas propiedades, y es igual de único que el objeto real todo esto ofrece al usuario: Los datos médicos pueden ser leídos y compartidos con total certeza de su integridad. En cada fase de la transacción o consulta tenemos a nuestra disposición la "trazabilidad de dato" podemos saber qué ha ocurrido o ha sido aportado en su paso por cualquier agente (nodo) de la cadena, además el paciente puede pasar a ser dueño de sus propios datos de salud, podrá acceder a ellos (historiales, citas, dolencias, tratamientos) en cualquier momento, gracias a su sofisticada codificación podrá mantener por completo la privacidad en el historial clínico siendo además un instrumento eficaz contra hackers y un aliado para el intercambio entre proveedores de salud y aseguradoras apuntando a un ecosistema sanitario global y participativo de esta forma la innovadora tecnología blockchain soluciona cualquier altercado que se presente en la red de datos clínicos.

1.4 Objetivos

1.4.1 Objetivo general

Desarrollar un prototipo de una plataforma de registro de historias clínicas basada en Tecnología Blockchain en el Hospital San Juan De Dios de Pamplona.

1.4.2 Objetivos específicos

Desarrollar un estado del arte sobre la aplicación de la tecnología Blockchain en el área de salud a nivel nacional e internacional.

Diseñar el modelo de transacción basado en tecnología Blockchain aplicable en el registro de historias clínicas.

Desarrollar el prototipo de la plataforma digital de registros médicos basados en transacciones mediante la tecnología Blockchain.

Marco teórico

Este capítulo muestra una vista teórica de la tecnología blockchain, orientada al diseño y arquitectura de las bases de datos distribuidas a nivel general y directamente relacionada con las historias clínicas, por medio del marco teórico se define precisamente las características del diseño y desarrollo de un prototipo basado en blockchain, únicamente los términos complementarios y asociados a la proyección de modelo tecnológico.

La tecnología blockchain es de los mayores descubrimientos del siglo XXI, dado el efecto que tiene en múltiples sectores desde el financiero hasta la salud y educación lo que muchos desconocen es que su historia se remonta a los años 90, pero no es sino hasta hace algunos años que empieza a popularizarse con una serie de aplicaciones que están surgiendo, resaltando el impacto que está destinado a tener a medida que la carrera por la digitalización aumenta. (RODRIGUEZ, 2018)

A mediados del siglo XX, varias iniciativas sentaron las bases de la criptografía, Según la **Real Academia Española** (**RAE**) se define como “el arte de escribir con clave secreta o de un modo enigmático”; varios años después, se han desarrollado una serie de algoritmos para permitir la creación de "criptografía de clave pública", Ahora se llama "blockchain" y su criptomoneda más popular es el "bitcoin".(Chari, 2020)
La criptografía es muy importante en la cadena de bloques. En la Blockchain los usuarios comparten información de forma cifrada. El ejército en la Segunda Guerra Mundial fue el primero en cifrar información con fines militares. (Chari, 2020)

El matemático británico Alan Turing logró descifrar el código emitido por la máquina "enigma" utilizada por los alemanes para comunicarse durante la Segunda Guerra Mundial, lo que supuso una gran ventaja para los Aliados. A partir de la década de 1970, un grupo de investigadores llevó a cabo una investigación para hacer que las comunicaciones mediante criptografía tuvieran más libertad. A partir de este momento, se comenzó a sentar la base de conocimiento de blockchain y diferentes criptografías. (Chari, 2020)

En 1998, el ingeniero informático chino Wei Dai desarrolló una solución en la que se utilizará "criptografía de clave pública" para realizar pagos electrónicos muy necesarios.

Este trabajo se realizó varios años después, más precisamente en 2008, para alguien con el seudónimo de Satoshi Nakamoto, escribió un artículo en la lista criptográfica de metzdowd.com en el que describía el protocolo Bitcoin. La red Bitcoin P2P se lanzó el 3 de enero de 2009, el primer cliente, el código abierto y la creación de la primera moneda virtual comenzaron a operar. (Chari, 2020)

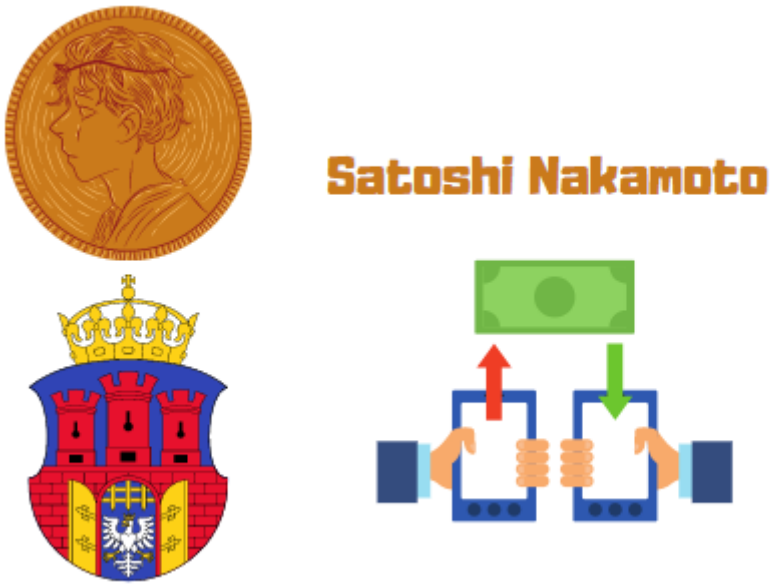


Figura 2.1 Primera aparición de blockchain con Satoshi Nakamoto

2.1 ¿Cómo surgió blockchain?

Stuart Haber y W. Scott Stornetta tuvieron la visión de lo que muchas personas han llegado a conocer como blockchain en 1991. Su primer trabajo consistió en proyectar una cadena de bloques protegida criptográficamente en la que nadie podía manipular las marcas de tiempo de los documentos sin embargo es en 2008 que la Historia de Blockchain comienza a ganar relevancia, gracias al trabajo de una persona o grupo conocida bajo el seudónimo de Satoshi Nakamoto. (RODRIGUEZ, 2018)

Satoshi Nakamoto es acreditado como el cerebro detrás de la tecnología blockchain. Se sabe muy poco acerca de Nakamoto solo que desarrolló la primera aplicación de la tecnología de registro digital.

La historia y evolución de blockchain no se detienen con Ethereum y Bitcoin. En los últimos años, una serie de proyectos han surgido aprovechando todas las capacidades de la tecnología de blockchain. (RODRIGUEZ, 2018)

El principal beneficio que nos brinda blockchain es la "desintermediación", es decir, la eliminación de intermediarios en un determinado proceso, y la eliminación de intermediarios en general cuando se introduce en ese momento el custodio o garante de su integridad y confiabilidad. Estos intermediarios son los certificadores actuales, operan de

manera garantizada y confían en ellos para asegurar el proceso de transacciones de activos con terceros.
La desventaja es que, en la mayoría de los casos, estos intermediarios asignàran o depositarán obligatoriamente los activos que administran (tokens en términos de blockchain) y los supervisarán. También introducen las condiciones, comisiones, operaciones, requisitos y los costos, el tiempo generalmente soportado si el token se va a utilizar para operaciones. (Valiente, 2018)

2.2 Bitcoin

La moneda más famosa y más utilizada del mundo; esta moneda creada en 2008 utiliza un sistema peer-to-peer (P2P) para intercambiar monedas virtuales. Por lo tanto, su diseño está "descentralizado y protegido a través de una sólida tecnología de cifrado. Este nuevo tipo de moneda ya no es una moneda física, pero puede resistir la corrupción y la manipulación".
En la mayoría de los casos, cuando los usuarios quieren usar Bitcoin para transacciones, no hay intervención de terceros, por lo que el costo es cero. Además, al utilizar este sistema de pago "es imposible manipular el valor de bitcoin o generar inflación produciendo más moneda. La propia red es una red que gestiona la transacción y emisión de bitcoins, y estos bitcoins se extraen mediante la llamada minería". Producido de forma controlada y descentralizada.
Como el precio de Bitcoin ha sido bienvenido por la demanda año tras año, el precio de Bitcoin se ha disparado y superó la marca de $10,000. Incluso para los fundadores, esta cifra era inimaginable hace unos años. (Chari, 2020)

2.3 Ethereum

Esta criptomoneda utiliza moneda de pago digital e Implementar contratos inteligentes, "una especie de software programado, Como cualquier otro software, realice algunas de las siguientes tareas o una serie de tareas Según la descripción introducida anteriormente "Estos archivos digitales se pueden utilizar cuando la empresa contrata personas.
Un acuerdo de uso de vivienda entre el propietario y el inquilino o Las personas que brindan el servicio y otras aplicaciones. "El diseño e implementación de Ethereum es completamente independiente de la criptomoneda Bitcoin", por lo que se considera que Ethereum es independiente de los pagos virtuales y presta más atención a las transacciones de datos. (Chari, 2020)

2.4 Blockchain

Es un sistema de libro mayor distribuido que puede registrar de manera efectiva las transacciones entre dos partes. Cada transacción se almacena en un libro mayor, y luego estos registros llamados bloques se conectan mediante una contraseña para formar una lista o área de bloques" Cadena de bloques". Este es un negocio descentralizado y también puede ayudar a administrar datos. Cada bloque de la red blockchain contiene datos de transacciones, hash criptográfico, hash de bloque anterior y marca de tiempo. El diseño de la cadena de bloques hace que los bloques sean resistentes a modificaciones. (Sharmaa & Prof. B. Balamurugan, 2020).

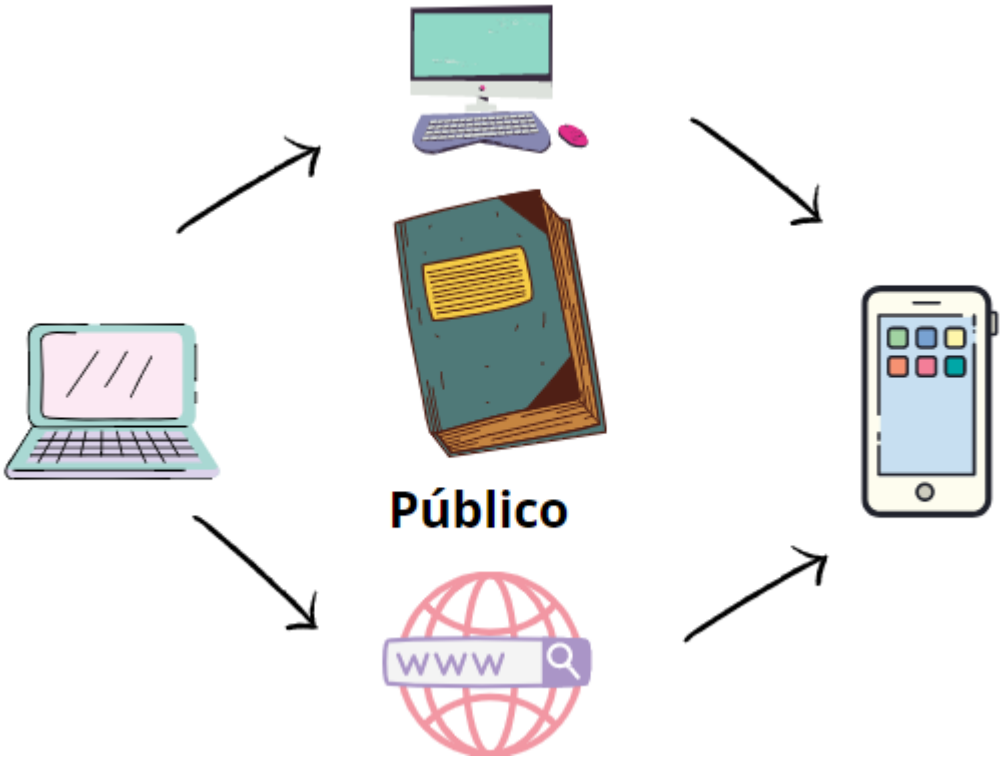


Figura 2.2 Modelo libro púbico de contabilidad

Los inicios de Blockchain se dan con la primera aplicación importante que es Bitcoin. Satoshi Nakamoto fue el creador de la primera moneda virtual y mencionó un nuevo sistema de efectivo electrónico. Esto es peer-to-peer y no requiere un tercero de confianza. Un año después en 2009, nació Bitcoin con este fin, combina herramientas de cifrado establecidas con métodos de cálculo para que las redes públicas de participantes que no

necesariamente confían entre sí, puedan acordar una y otra vez que el libro de contabilidad compartido refleja los hechos. (Cies et al., 2020)

“Blockchain es una tecnología de base de datos descentralizada y distribuida que permite mantener un registro creciente de transacciones mediante encriptación y otras actividades, verificando su permanencia e historia de cambios” (García-Morales, 2018)

Blockchain se utiliza para transacciones seguras a través de la red. Desde que surgió la idea de la tecnología en 2008, el interés en la tecnología blockchain y sus aplicaciones ha ido en aumento. La razón del creciente interés en la tecnología blockchain es que no está sujeta a la autorización centralizada que proporciona. La seguridad, transparencia e integridad de los datos, sin ninguna interferencia de organizaciones de terceros que administran transacciones, brindan oportunidades atractivas para la investigación en varios campos. (Sharmaa & Prof. B. Balamurugan, 2020)

Diez años después, la madurez de la tecnología blockchain ha abierto horizontes futuros para el funcionamiento de varias industrias en el mundo. Hoy en día, blockchain tiene aplicabilidad en las siguientes áreas:

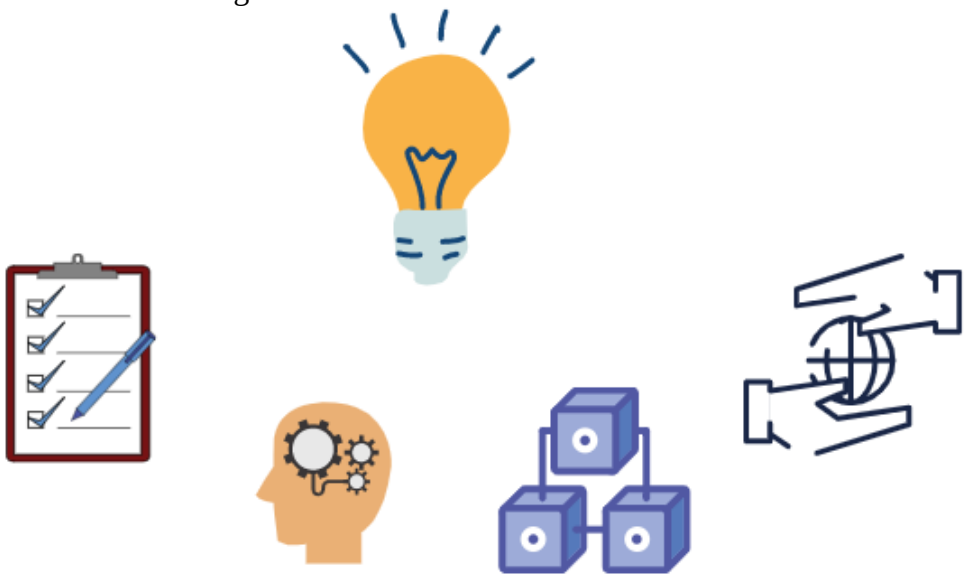


Figura 2.3 Aplicaciones blockchain

• Depósito de transacción, contrato garantizado, arbitraje de terceros y aprobación de la transacción.
• Transacciones financieras: criptomonedas, capital privado, crowdfunding, derivados, rentas, pensiones.

• Registros públicos: derechos de propiedad, registro de vehículos, licencia comercial, certificados de matrimonio y defunción
• Prueba de identidad: permiso, identificación personal, pasaporte, registro de voto político.
• Registros privados: préstamos, contratos, apuestas, firmas digitales, testamentos, fideicomisos
• Internet de las cosas (IoT).
• Servicios financieros.
• Propiedad inteligente.
• Atención sanitaria inteligente.
• Gobierno inteligente.
(C. Chisaba, 2017)

Blockchain es una base de datos que puede ser compartida directamente entre sí por una gran cantidad de usuarios, permitiendo que la información se almacene de manera inmutable y ordenada; la creación de una poderosa blockchain debe garantizar dos propiedades básicas "

1. Disponibilidad: para garantizar que las transacciones honestas sean enviadas en la blockchain se ha agregado condiciones específicas a la cadena de bloques para evitar que los nodos dañados denieguen el servicio (Denegación de servicio, DoS).
2. Persistencia: Cuando el nodo estabiliza la transacción, los nodos restantes (si son honestos) verificarán que la transacción es estable, para que no se puedan realizar modificaciones futuras. (Chari, 2020)

2.5 ¿Cómo se forma la cadena de bloques?

Consiste en una red de grandes computadoras conectadas a los llamados nodos. Blockchain es un grupo de nodos conectados a una red descentralizada. Un protocolo estándar para verificar y almacenar la misma información de registro en una red P2P, para que todos puedan intercambiar bienes y servicios sin terceros. En otras palabras, blockchain también se llama blockchain, es una tecnología que permite el mantenimiento de bases de datos distribuidas entre redes informáticas. Esta información está asegurada por el hecho de que se distribuye por todo el sistema, lo que evita que se modifique sin el consentimiento de otras computadoras. (Cies et al., 2020)

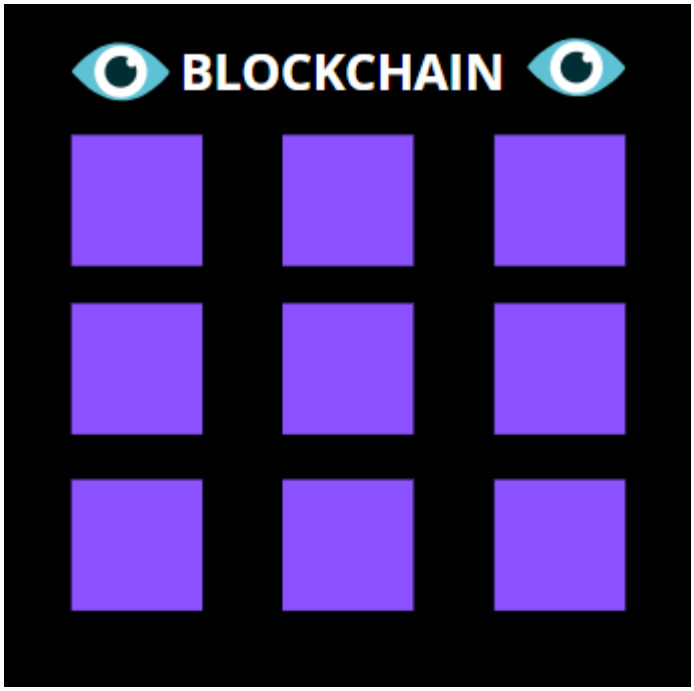


Figura 2.4 Bloque contenedor de blockchain

Una base de datos distribuida es una base de datos que se utiliza junto con una sola base de datos instalada en una serie de computadoras específicas (nodos) distribuidas por diferentes regiones geográficas, y no depende de una sola unidad de procesamiento.

Para comprender cómo funciona una red blockchain típica, pensamos que un grupo de nodos (clientes) que se ejecutan en una sola cadena de bloques forma una red P2P. La secuencia de pasos involucrados se enumera a continuación

- ✓ Paso 1: El usuario usa su clave privada / pública para interactuar con la cadena de bloques. Estos usuarios hacen que sus claves públicas sean direccionables en él y usan sus claves privadas para firmar transacciones. La transacción firmada se puede transmitir a los colegas en un solo paso. El cifrado de clave asimétrica ayuda a mantener la integridad, la verificación de identidad y el no repudio dentro de la red.

- ✓ Paso 2: Los vecinos verifican la validez de la transacción de igual a igual, descartan las transacciones no válidas y luego envían las transacciones válidas. Utiliza reglas relacionadas con la aplicación (ciertas condiciones que debe cumplir cada transacción de la base de datos) programadas en el cliente para verificar la validez de la transacción.

- ✓ Paso 3: Extrae las transacciones verificadas recopiladas dentro del tiempo acordado (es decir, empaquetadas con la fecha y la hora). Según la estrategia de consenso, se

seleccionan nodos de minería para transferir estos bloques de marca de tiempo a toda la red.

- ✓ Paso 4: El nodo verifica si el bloque propuesto ha sido cotizado por el valor hash de su bloque anterior y mantiene una transacción válida. Si sigue siendo verdadero, el bloque se agrega a la cadena, pero se descarta. (Bhushan et al., 2020)

2.6 Diferencias entre las cadenas de bloques y las bases de datos

En términos de aplicaciones de la tecnología de cadenas de bloques, se podría argumentar que aún estamos en la fase de exploración. Es prudente ser cauteloso con las afirmaciones de que esta tecnología en particular en su cadena de bloques permitida, podría perturbar los datos como los seguros bancarios, la contabilidad y salud. En particular, sería útil explorar exactamente qué ventajas tienen las cadenas de bloques en comparación con las tecnologías de registro de transacciones bien conocidas como las bases de datos para empezar proporcionamos una breve descripción sobre los tipos y capacidades de las bases de datos modernas, dependiendo de la naturaleza de los datos que se almacenan. (Valiente, 2018)

2.7 Libro mayor distribuido

Es una estructura de datos replicada en todos los nodos de la red y contiene una lista ordenada de transacciones agrupadas y enlazadas en un bloque. El historial de todas las actualizaciones realizadas al estado inicial de la cadena de bloques se registra en el libro mayor. La aplicación encriptada utiliza un modelo de cuenta de usuario similar a los sistemas bancarios tradicionales. El sistema puede conectar varios libros de contabilidad en una cadena de bloques común, al igual que en una gran empresa, especificando un libro de contabilidad independiente para cada departamento.

Los activos digitales son emitidos por entidades del mundo real, su intercambio y existencia se registra mediante blockchain, mientras que la criptografía obtiene su valor directamente de blockchain. Corda, Multichain y BigchainDB proporcionan libros de contabilidad para el seguimiento e historial de productos de la tienda. Utilizan un modelo de datos basado en transacciones para activos. El entorno privado es el objetivo de estos sistemas, en los que muchas organizaciones intercambian activos entre sí. (Sharmaa & Prof. B. Balamurugan, 2020)

Blockchain se compromete a mejorar la atención al paciente y aumentar la exhaustividad de los datos, Distribuir información, reduciendo así el costo de cada transacción. Buscar integrar y mantener la información en el sistema de salud.

Las ventajas que aporta la tecnología blockchain en el ámbito de la salud son las siguientes:

- ✓ Todos los participantes sanos pueden acceder a su información de manera segura y confiable.
- ✓ Los datos están dispersos, lo que significa que todos pueden acceder información, además, los requisitos físicos no serán tan costosos porque la información se distribuirá.
- ✓ Los identificadores públicos y privados de cada paciente estarán encriptados, creando una forma más segura de proteger la información.
- ✓ La información se comparte en todo el sistema.
- ✓ Los contratos inteligentes le permiten configurar la información del paciente para que determinadas entidades puedan verla.
- ✓ Intercambio de información médica y accesibilidad de registros médicos.
- ✓ Transparencia a la hora de modificar la información, pues esto debe ser acordado por cada participante de la red "entidad sana"

A largo plazo, la red blockchain de registros médicos electrónicos nacionales puede que mejore la eficiencia y brinde a los pacientes mejores resultados de salud; sin embargo, no es una tecnología completamente madura y, por lo tanto, no puede aplicarse de inmediato. Antes de que las organizaciones de atención médica puedan aplicar la tecnología blockchain en todo el país, se deben abordar varios desafíos económicos, técnicos, organizacionales y de comportamiento. (Quiroga Cruz, Jorge; Cubillos Herrera, 2018).

El sistema blockchain utiliza una tecnología de cifrada pesada para garantizar la integridad del libro mayor (verifique la capacidad de los datos para operar en blockchain). Por lo tanto, en un entorno público donde no existe una confianza preestablecida en la blockchain publica, el libro mayor debe poder evitar el problema del doble gasto, por lo que se debe realizar la protección de la integridad. También es necesario en blockchain privados, porque a veces los nodos autenticados en blockchain privados también pueden tener un comportamiento malicioso.

El plan de protección de integridad de datos es aplicable a los sistemas blockchain. En el primer esquema, el árbol hash de Merkel se utiliza para proteger el estado de almacenamiento global del hash raíz en el bloque. (Sharmaa & Prof. B. Balamurugan, 2020)

La cadena de bloques contiene datos estructurados que agregan las transacciones que están disponibles públicamente en el libro mayor público (cadena de bloques). No importa lo que se utilice, las características de blockchain son:

1. Utiliza tecnología de encriptación para proteger la cadena y sus datos de transacción (seguridad de la red) De igual forma, integra conceptos como teoría de juegos y redes P2P para verificar el consenso de diferentes transacciones.
2. Su estructura está dispersa. Esto permite a todos los usuarios vinculados a la cadena de bloques aprobar y verificar transacciones.
3. Evita cambios en la información registrada.
4. Registra todas las transacciones creadas en la cadena de bloques.
5. Se convierte en un libro de contabilidad digital.
6. Registra las transacciones en orden cronológico.
7. Permite que la información sea abierta, transparente, verificable y auditable.
8. Reduce la dependencia de terceros.
9. Permite la trazabilidad y el almacenamiento. (C. Chisaba, 2017)

2.8 Gestión de la identidad

El certificado de clave pública del usuario lo identifica de forma única en la cadena de bloques. Inicialmente, el usuario genera la clave de acuerdo con la curva elíptica. Luego, el hash se deriva como su identidad y se utiliza como número de cuenta o dirección de transacción en el sistema de cifrado. El usuario firma la transacción con la clave privada para declarar la propiedad de la transacción. También hay una capa de control de acceso. Proporcionar servicio de autoridad de certificación o servicio de proveedor de membresía. Los administradores pueden utilizar estos servicios para Implementar estrategias arbitrarias para controlar el acceso a la cadena de bloques. (Bhushan et al., 2020)

"En la actualidad, el sistema de salud colombiano exige nuevos retos y compromisos. La innovación y reestructuración de los centros de salud implican un reconocimiento holístico de las necesidades en el área". (C. Chisaba, 2017)
Actualmente, el sistema de salud de Colombia requiere nuevos desafíos y compromisos. La innovación y reorganización del centro de salud significa un conocimiento global de las necesidades en esta área: infraestructura, servicios, gestión, rentabilidad, optimización, cobertura, portabilidad, transparencia, etc. La tecnología Blockchain se encuentra en un importante período de desarrollo, en Colombia es necesario fortalecer el desarrollo de blockchain para satisfacer las necesidades locales. En el sector de la salud, la tecnología blockchain aparece en todos los niveles de actividades comerciales del departamento. Por ejemplo, en la cadena de valor del sector salud, encontramos la industria farmacéutica, la distribuidora farmacéutica IPS (Institución Prestadoras, EPS (Health Provider Company), hospitales, clínicas, gremios y empresas de personal médico, droguerías y farmacias, distribuidores de equipos biomédicos, empresas de software médico, empresas de servicios generales y sanitarios (abastecimiento y recogida de residuos hospitalarios), Empresas de infraestructura médica, ambulancias, etc. Todos estos participantes requieren seguridad general, confidencialidad y confianza en la información compartida. (C. Chisaba, 2017)

2.9 Aplicabilidad de blockchain

Puede comenzar desde el nacimiento de una persona e incluso generar identidades digitales y comenzar a almacenar información sobre los recién nacidos, las enfermedades y el historial médico de los padres; mapeo integración de identidad genética y digital todo el personal médico, proveedores Drogas y otras partes interesadas. Hasta cierto punto, la gente puede llevar el centro médico hasta su casa (portátil) e ingrese la información de salud de los miembros de la familia, informe de emergencias o medicamentos insuficientes en tiempo real y consulte a un médico esas necesidades inmediatas. No cabe duda de que la ventaja radica en Blockchain, porque la trazabilidad de la salud de las personas se Garantiza, se protege, se comparte y todo ello fortalece la gestión de la salud ciudadana. (C. Chisaba, 2017)

2.10 Seguridad basada en cadenas de bloqueo

Siempre que un adversario tenga la intención de gastar dos criptomonedas o robar una criptomoneda el atacante debe generar un bloqueo mediante un libro a largo plazo. Si un nodo de red legítimo no puede extraer o generar bloques más rápido que otros nodos, no aceptará el bloqueo del oponente. Si el bloque recién generado alcanza más de la mitad de la potencia informática total, el atacante puede fusionarlo en una cadena de bloques a largo plazo. Sin embargo, técnicamente hablando, no es fácil para los oponentes hacerlo. Blockchain integra cuatro tecnologías claves, red P2P, contrato inteligente, cifrado asimétrico y libro mayor distribuido. Estas tecnologías han promovido blockchain como una nueva generación de procesamiento de información inteligente, eficiente, justo, abierto, confiable y seguro. Estas técnicas se discutirán en las siguientes subsecciones. (Bhushan et al., 2020)

2.11 Red P2P

En las aplicaciones P2P distribuidas, los colegas colaboran y se organizan para completar tareas como cargar datos, pasar mensajes y reenviar archivos. La cadena de bloques utiliza una arquitectura de red P2P descentralizada, con equilibrio de carga y tolerante a fallas, en lugar del modelo tradicional cliente-servidor. De acuerdo con la arquitectura y el diseño de la red, estas redes P2P se dividen en no estructuradas, híbridas y estructuradas. Varios trabajos han demostrado que la red real es similar a un modelo de mundo pequeño con una longitud de camino promedio más pequeña y un coeficiente de agregación mayor. La red blockchain también se opera y diseña de acuerdo con el modelo de mundo pequeño, entre ellos, los nodos de la red se pueden dividir en series de nodos grabados y no grabados según su capacidad de grabación. Bajo diversas condiciones de nodo cambiantes, el modelo de mundo pequeño puede garantizar dinámicamente la estabilidad de la red. También mejora la solidez general de la red blockchain y preserva la consistencia e integridad de los datos de las transacciones. Además, los mineros y usuarios del sistema blockchain P2P pueden

coludirse entre sí o mostrar un comportamiento egoísta. Él y otros propusieron integrar estrategias de precios de seguridad y métodos de verificación en los mecanismos de incentivos. La arquitectura propuesta se enfoca en brindar recompensas a los usuarios para compensar los recursos que consumen. Este mecanismo de incentivos se introduce para satisfacer las diversas necesidades de los usuarios en un entorno P2P distribuido y dinámico**.** (Bhushan et al., 2020).

2.11.1 Red distribuida

Una red distribuida es una topología de red, que se caracteriza por no tener un centro individual o colectivo. Figura 2.5 Estos nodos están vinculados entre sí, por lo que ni siquiera tienen un grupo estable y no pueden filtrar la información que se transmite en la red. Como resultado, desaparece la línea divisoria entre el centro característico y la periferia de las redes centralizadas y descentralizadas.

El desarrollo de medios electrónicos personales para la edición y publicación llevaron a la aparición de Blogosphere (el primer medio de comunicación distribuido). Un sistema distribuido no es más que un grupo de computadoras que trabajan juntas de manera coordinada intercambiando mensajes para lograr metas. En tal sistema, los estados y programas se almacenan en todas las computadoras de la red, lo que brinda autonomía en la operación y seguridad en el registro de información confidencial ya que no es controlada por algún agente externo ni está almacenada en elementos de red fuera del control de los dueños de la data que fluye.

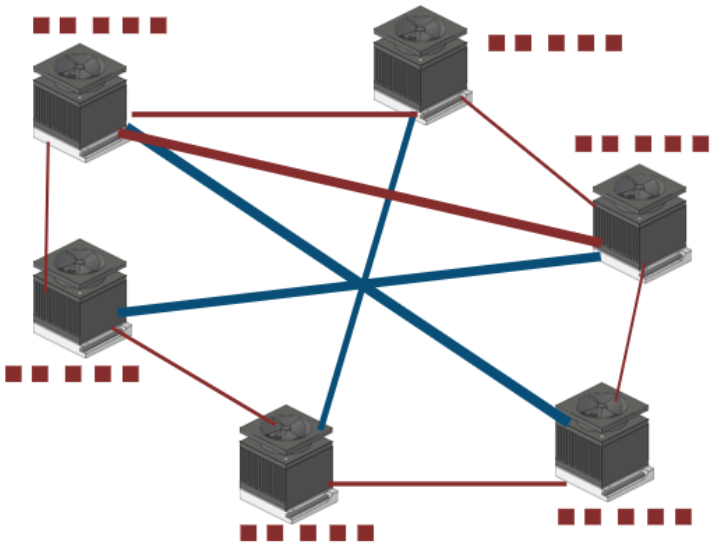


Figura 2.5 Red distribuida

2.12 Encriptación asimétrica

La tecnología básica para utilizar dos claves diferentes para mejorar la seguridad de la cadena es: clave privada y clave pública. Las dos contribuciones principales del cifrado asimétrico a la cadena de bloques son las firmas digitales y el cifrado de datos. Además de verificar y firmar transacciones, la criptografía asimétrica también se puede utilizar para cifrar los datos de blockchain registrados. El token tiene una clave pública y puede ser visto por todos, mientras que la clave privada puede usarse para operaciones de autorización. Aitzhan y otros han propuesto una herramienta eficaz llamada tecnología de firma múltiple. Lo importante es que los datos registrados en el bloque deben ser verificados por el nodo de red en el blockchain. La tecnología de firma ciega se utiliza para lograr los objetivos de seguridad y evitar la fuga de información. Las firmas digitales se pueden utilizar para firmar transacciones de forma más segura, y muchas criptomonedas también utilizan firmas digitales. Estos se pueden usar en combinaciones y contratos de múltiples firmas, porque requiere firmas digitales con diferentes claves privadas antes de iniciar cualquier medida de cumplimiento. (Bhushan et al., 2020)

Desafíos de blockchain y direcciones futuras además de los muchos beneficios que brinda la tecnología blockchain, existen pocos desafíos que limitarán su utilidad en muchas de las aplicaciones de seguridad discutidas en las secciones anteriores. Algunos de estos desafíos se detallarán en las siguientes subsecciones. (Bhushan et al., 2020)

2.13 Privacidad y anonimato

La mayor ventaja y característica del uso de la tecnología blockchain es que proporciona un pseudo anonimato muy necesario para los usuarios, porque las blockchains públicas son vulnerables a los ataques debido a su apertura. Blockchain permite la seguridad, pero la interacción entre estas entidades tiene un propósito común, pero no confían entre sí. La autorización de blockchain tiene varias limitaciones, como la incapacidad para procesar una gran cantidad de transacciones, la necesidad de escribir contratos inteligentes en un dominio de lenguaje específico, la incapacidad de admitir transacciones no deterministas y el rendimiento limitado debido a la ejecución secuencial y transaccional. La mayoría de los programas existentes solo pueden proporcionar un cierto grado de anonimato, por lo que se necesita más investigación para desarrollar un método completamente anónimo para satisfacer las necesidades de varias aplicaciones de seguridad. (Bhushan et al., 2020)

2.14 Nodos de computación y minería

Los servicios de seguridad utilizados y el proceso de extracción relacionado con la tecnología blockchain requieren muchos cálculos en el proceso de generación de firmas, cifrado y descifrado. Con este fin, se han realizado varios trabajos de investigación

dedicados a las estrategias de asignación de recursos en el proceso de extracción de bloques. Además, para reducir los requisitos computacionales para la firma y el cifrado de datos, se necesita más investigación para desarrollar un esquema criptográfico simple. (Bhushan et al., 2020)

2.15 Gastos generales de comunicación y almacenamiento

Debido a la naturaleza altamente dinámica de las aplicaciones actuales, los datos de origen y las listas de acceso deben cambiarse con frecuencia. Por el contrario, debido a que la tecnología blockchain es una red de igual a igual, generará una gran cantidad de gastos generales en términos de capacidades de procesamiento del sistema y la red. Estos gastos generales de procesamiento y almacenamiento crean otros problemas en la adopción de blockchains para diversas aplicaciones de seguridad. Este problema se agrava aún más cuando se implementa la cadena de suministro blockchain o cualquier otra aplicación similar de uso intensivo de datos. Algunas de las soluciones propuestas se basan en compartir actividades de transacciones de la cadena de bloques principal mediante el uso de redes de canales de pago. Sin embargo, esto oculta la transparencia de los datos y compromete la privacidad. Esto requiere encontrar soluciones más efectivas en este sentido. (Bhushan et al., 2020)

2.16 Consultar los datos almacenados en los bloques

Las aplicaciones existentes basadas en blockchain se enfocan en reducir el fraude, aumentar la resistencia a la manipulación, reducir los costos operativos y ejecutar contratos. Sin embargo, la cadena de bloques admite una capacidad de consulta limitada y puede marcarse como una base de datos distribuida infalsificable centrada en el almacenamiento de datos. Blockchain utiliza el protocolo de consenso y la tecnología de cadena hash para garantizar la integridad de los datos. Impulsadas por la procedencia y la naturaleza descentralizada de blockchain, estas soluciones de seguridad protegidas por contraseña destacan su potencial para innovar los sistemas de bases de datos tradicionales. Con la adopción de la tecnología blockchain aumentando exponencialmente
Para aplicaciones con uso intensivo de datos, como la gestión de propiedad intelectual, la cadena de suministro y las finanzas, se ha mejorado la tasa de utilización. Consultar solicitud de datos de almacenamiento. Para ejecutar estas consultas, el sistema requiere que todos los nodos pares recorran todos los registros y generen el resultado final de la consulta. Este proceso de recuperación de registros aleatorios requiere mucho tiempo para procesar la consulta incluso si Blockchain ofrece muchas ventajas de seguridad, búsqueda de registros efectiva y seguimiento de transacciones de datos actuales en blockchain. (Bhushan et al., 2020)

2.17 Algoritmo de consenso

Cada bloque agregado en la cadena de bloques tiene que pasar por un proceso para obtener el protocolo de todos los demás nodos que se han registrado en la red, es decir, el nodo agregado es un nodo autorizado. Utilice un algoritmo de consenso para realizar este proceso. Ayudan a lograr la confianza entre los participantes y la confiabilidad en la red. (Sharmaa & Prof. B. Balamurugan, 2020)

El protocolo de consenso debe poder lidiar con estos fracasos bizantinos. Los sistemas Blockchain incluyen una gran cantidad de protocolos de consenso, que van desde protocolos restringidos por comunicaciones (como Byzantine Practical Fault Tolerance (PBFT)) hasta protocolos restringidos por computación (como PoW). Entre estos dos extremos, existen muchos acuerdos híbridos destinados a mejorar la actuación. (Bhushan et al. 2020).

El protocolo de consenso en blockchain tiene 2 retos:

1) Atacantes
   Las redes tecnológicas poseen el problema de ser blanco de hackers, personas maliciosas que buscan perturbar sistemas ajenos para beneficiarse con fines lucrativos o personales, el algoritmo de consenso es la solución a dicho problema pues mediante una prueba despliega los bloques dentro de blockchain, una vez esté validado lanzan la petición a los mineros quienes se encargan de establecer este bloque dentro de la cadena, es allí cuando los hackers intentan atropellar la cadena y si la logran romperla ya los demás nodos de la red conocen la estructura de este bloque lo que ocasiona que no cumpla con el enlace de la secuencia de la red considerando los bloques siguientes como ajenos a la misma, los nodos a través de consenso se comunican y comparan la longitud de cada cadena la cual puede haber sido descompuesta por un ataque, el consenso determina que en algún nodo la cadena está alterada por lo tanto reemplaza por la cadena de mayor longitud. Los ataques tendrías que llevarse a cabo por todos los nodos en su totalidad lo que es lógicamente y físicamente imposible
2) Competencia entre cadenas

   - En una cadena de bloques grande distribuida por muchos lugares, podemos encontrar lag entre nodos, especialmente los que se encuentran a largas distancias los unos con los otros.

   - Puede ocurrir que 2 nodos que están a larga distancia debido al lag puedan minar un bloque al mismo tiempo.

- ❖ Minar consume recursos como CPU, electricidad y más que el algoritmo es proof of work se ha tenido que pagar por todo eso.

- ❖ La cadena más larga se reemplaza en los demás nodos.

Cuando hay duplicados se espera a que se añada otro bloque.

Los algoritmos de consenso comúnmente utilizados son PoW, PBFT, PoS

En la red blockchain, no existe una institución central y confiable. Por lo tanto, llegar a un consenso sobre estas transacciones entre los nodos que no son de confianza en una red distribuida es un tema importante. Diseñó una serie de acuerdos para llegar a consensos antes de vincular nuevos bloques en la cadena de bloques, entre todos los nodos distribuidos. (Shuyun Sh, 2020)

2.17.1 PoW

Es el mecanismo de consenso utilizado en Bitcoin. Si un nodo de minería con ciertas capacidades informáticas (hash) espera obtener algunas recompensas, los mineros deben realizar tareas de minería difíciles para demostrar que no es malicioso.

Esta tarea requiere que los nodos realicen repetidamente cálculos hash para encontrar un valor Noce calificado, que cumpla con el requisito de que el encabezado del bloque hash debe ser menor (o igual al valor hash del objetivo). Los números aleatorios son difíciles de generar, pero muy fáciles de validar para otros nodos debido al difícil número de cálculos, esta tarea es muy costosa (en términos de recursos informáticos).

Un ataque del 51% es un ataque potencial a la red blockchain. Si un minero o un grupo de mineros pueden controlar más del 51% de la potencia de cálculo, pueden interferir con la generación de nuevos bloques y crear transacciones a favor del registro fraudulento por parte del atacante. (Shuyun Sh, 2020)

2.17.2 PoS (Proof of Stake)

Es un mecanismo de ahorro de energía mejorado de PoW. Se cree que los nodos con un mayor número de apuestas (como monedas) tienen menos probabilidades de atacar la red. Sin embargo, es injusto elegir según el saldo de la cuenta porque es más probable que el nodo más rico se convierta en el nodo dominante en la red, que es similar a un sistema gradualmente centralizado

PBFT (Practical Byzantine Fault Tolerance) es un algoritmo de replicación que tolera errores bizantinos e incluye un protocolo de tres fases. Prepárate, practica y participa en

estas tres etapas. Si un nuevo bloque ha recibido respuestas válidas de más de 2/3 de todos los nodos en cada etapa, está bien. En el caso de menos de 1/3 de los nodos espejo bizantinos maliciosos, se puede garantizar la corrección de toda la red. La estructura ultraligera permitida utiliza PBFT como algoritmo de consenso para verificar las transacciones. (Shuyun Sh, 2020)

El algoritmo de consenso tiene las siguientes características:

- ✓ Cada nodo de la red actúa como una entidad hipotecaria, lo que hace que los movimientos de transacción sean visibles para cada nodo.
- ✓ Consulte las reglas de cada transacción.
- ✓ Ejecutar el algoritmo.
- ✓ Compartir información.
- ✓ Los nodos restantes verifican y comparten información y llegan a un consenso.

En definitiva, el algoritmo de concesión es un proceso encargado de verificar características para compartir información, características que permiten a cada nodo de la red intervenir en el movimiento de las transacciones, actuar como testigos y juzgar cuándo completa la transacción. Cuando se cumple el contrato inteligente o las reglas de cada transacción, el algoritmo de concesión comienza a funcionar, incluyendo compartir información entre todos los nodos de la red. Una vez que la información ingresa a cada nodo, el algoritmo comienza a verificar si la información está acordada en cada nodo, y luego llega a un acuerdo o concesión para actualizarlo. (Quiroga Cruz, Jorge; Cubillos Herrera, 2018).

2.18 Registro inmutable

Una de las características que distingue al blockchain es su inmutabilidad, es evidente que una vez se haya minado un bloque dentro de blockchain es imposible modificar su contenido. La cadena de bloques es realmente un registro de datos inmutable por el complejo problema que suele ser vulnerar un bloque establecido a lo largo de la cadena, la inmutabilidad proporciona una estrategia y un proceso de gestión de acceso e identidad integral para el fortalecimiento de modelos blockchain perfecto para registros médicos a prueba de manipulaciones.

Es un objeto cuyo estado no se puede modificar una vez creado, si es cambiado ya no sería el objeto previamente establecido como registro, el resto de la red quedaría completamente descompensado lo que ocasiona una ruptura de la cadena como en la Figura 2.6

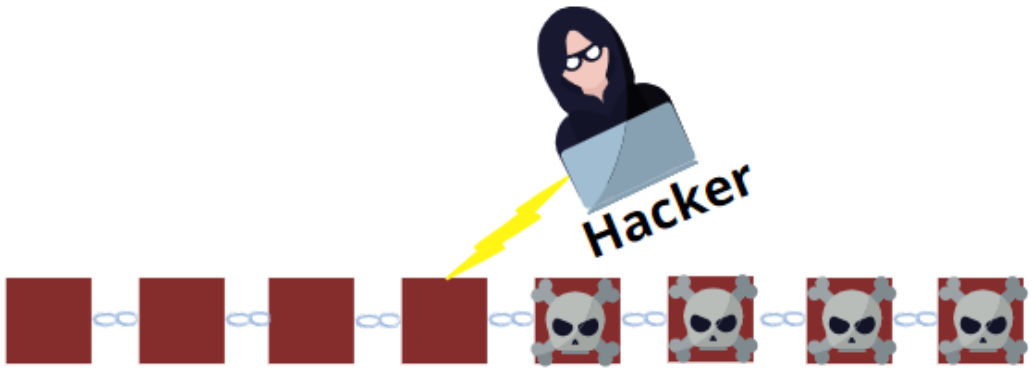


Figura 2.6 Registro inhackeable

2.19 Función hash

Una transacción es una unidad de datos que contiene detalles de la transacción y marcas de tiempo. Ambos pueden expresarse como números de computadora o cadenas. Puede pensar en la cadena de bloques como una tabla con tres columnas, donde cada fila representa una transacción diferente. La primera columna almacena la marca de tiempo de la transacción, la segunda columna almacena los detalles de la transacción y la tercera columna almacena el hash de la transacción actual. El valor más sus detalles más el valor hash de la transacción anterior. Cuando se inserta un nuevo registro en la cadena de bloques, el último valor de hash de la computadora se transmitirá a cada parte interesada. Cada parte no tiene que guardar una copia de todo el historial de transacciones, solo algunas partes pueden hacerlo. Como todo el mundo conoce el último hash, cualquiera puede comprobar que los datos no han sido modificados, porque sería imposible sin obtener otro hash, por tanto, no es válido. La única forma de cambiar los datos mientras se conserva el hash es encontrar conflictos en los datos, lo cual es computacionalmente imposible. (Pierro, 2017)

Detecta cualquier tipo de manipulación de la información almacenada en el bloque durante la búsqueda. En la cadena de bloques, esto se hace mediante una función hash.
Una función hash es una función que recibe información de cualquier tamaño y genera otra información de tamaño fijo a partir de ella, que generalmente se usa para identificar la entrada[input].
Las características de una función hash ideal son:

- ✓ Debería ser computacionalmente fácil de calcular. Incluso cambiar un poco de información debería cambiar completamente el hash.
- ✓ Debería ser imposible adivinar la información de entrada del hash y de salida.

- ✓ La transacción se almacena inicialmente en un conjunto de transacciones no confirmadas. El proceso de poner transacciones no confirmadas en bloques y calcular la prueba de trabajo se llama minería de bloques. Una vez que se cumplen las condiciones, se puede decir que el bloque ha sido extraído y colocado en la cadena de bloques. (Piedra, 2018)

Los mineros suelen ser premiados con alguna criptomoneda como una recompensa por usar su potencia de cálculo para calcular la prueba de trabajo. Así es como se ve nuestra función de minado. (Piedra, 2018).

2.19.1 SHA256

Es el algoritmo criptográfico que se está utilizando para cifrar la información. Si un bloque es alterado entonces el hash cambia ya no serían iguales, la cadena se rompe. Una función criptográfica hash usualmente conocida como hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

2.19.2 Hashing

Un hash es un proceso para crear un string único de caracteres de cada fuente de datos, contraseñas.etc
El output tiene una longitud fija definida por el algoritmo
El output cambia completamente si la fuente cambia
Usado mayormente para mantener la integridad de los datos y autenticación segura de contraseñas

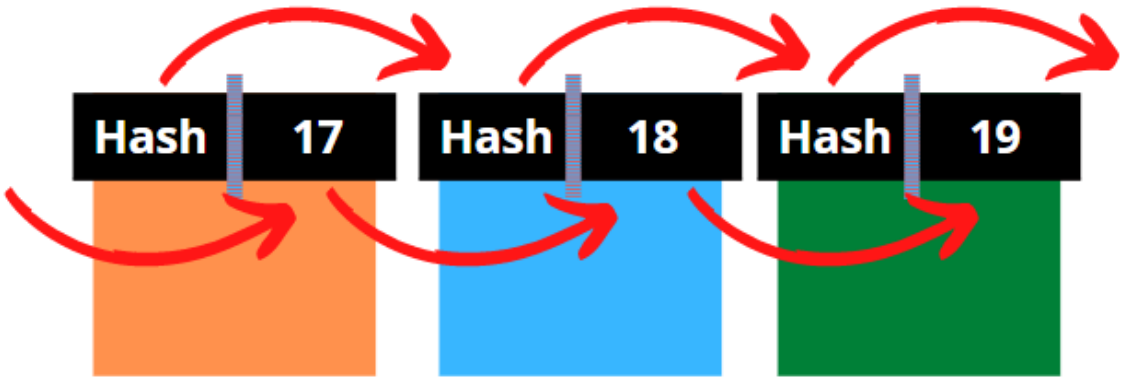


Figura 2.7 Bloques encadenados

Un protocolo es una manera definida en que se establece comunicación entre dispositivos como TCP, AIPE, HTTP.

- Colisiones de hash: Ocurre cuando dos pedazos de datos producen el mismo hash.
- Un buen algoritmo de hashing debe minimizar las colisiones.
- Crackear el hash significa deliberadamente cambiar el input data para que pueda ser igual al hash anterior.
- Las colisiones niegan la integridad de la información.

Algoritmos comunes de hash

Message digest family

- ✓ MD4 128 bits usado para hashear claves locales de Windows
- ✓ MD5 usado en varios sistemas de integridad de datos (craqueados)

Secure hashing algorithms

- ✓ SHA1 160bits usado como estándar de la industria(craqueados)
- ✓ SHA2 254,256,384 y 512 bits debería ser utilizado como mínimo (no craqueado)

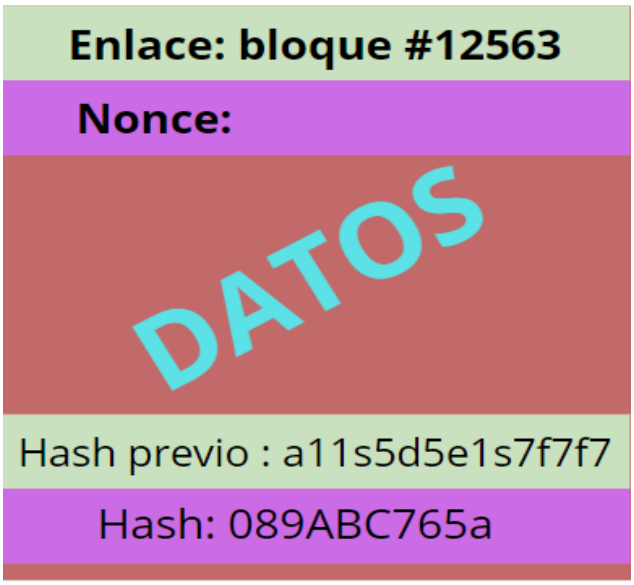


Figura 2.8 Bloque dentro de la caden

- ✓ Solo se puede cambiar el nonce

- ✓ Hash SHA256: un hash es un número hexadecimal de 64 bits, corresponde a número y letras de la A-F.

- ✓ La única forma de que los mineros obtengan la meta es cambiando el nonce y haciendo operaciones matemáticas obteniendo diferentes hashes hasta encontrar el que hemos puesto

- ✓ La meta es un algoritmo cuyos ceros son mínimo 4 inicialmente (mientas mas ceros hallan más difícil va ser poder mirarlo)

- ✓ Tolerancia bizantina de fallas (Todos deben estar de acuerdo)

2.20 Tipos de blokchain

Según los permisos otorgados a los nodos de la red, los sistemas blockchain se dividen en tres tipos

2.20.1 Public blockchain

La cadena de bloques pública está abierta a cualquiera que quiera unirse en cualquier momento y actúa como un simple nodo o como un minero para obtener recompensas económicas. (Bitcoin y Ethereum) son dos plataformas de cadenas públicas de bloques muy conocidas.

2.20.2 Private blockchain

Funcionan sobre la base del control de acceso, en el que los participantes deben obtener una invitación o permiso para unirse. Tanto GemOS como MultiChain son plataformas de blockchain privadas típicas.

2.20.3 La cadena de bloques del consorcio

La cadena de bloques del consorcio es "semiprivada" y se encuentra en la cerca entre las cadenas de bloques públicas y privadas. Se otorga a un grupo de organizaciones aprobadas generalmente relacionadas con el uso comercial para mejorar el negocio. La arquitectura Hyperledger es el marco de blockchain de las alianzas empresariales. Ethereal también apoya la construcción de blockchain de alianza. (Shuyun Sh, 2020)

2.21 Privacidad de datos en blockchain

Blockchain proporciona seguridad para la red mediante el uso de tecnología de cifrado. Cada bloque individual de la cadena de bloques está conectado a un bloque antes y después. Esto hace que sea difícil para un hacker manipular cualquier registro, porque el hacker también debe cambiar el registro o bloque asociado al registro que desea manipular o

acceder, lo cual es prácticamente imposible en una red enorme con grandes cantidades de datos. El número de bloques en la cadena de bloques. Cualquier blockchain comienza con un bloque de génesis, que es la base para agregar otros bloques en secuencia. Cada bloque de la cadena de bloques contiene el hash, la marca de tiempo y los datos de transacción del bloque anterior. Estos se utilizan para generar un hash de un bloque específico utilizando un algoritmo criptográfico. El hash es el identificador único del bloque en la cadena de bloques. Estos punteros hash también son responsables de vincular cada bloque a su predecesor y guardar el hash del bloque anterior. Debido a que cada bloque de la cadena de bloques está conectado al bloque anterior, la cadena de bloques se vuelve inmutable. (Sharmaa & Prof. B. Balamurugan, 2020)

Estos bloques están protegidos por contraseña. Los participantes de la red tienen sus propias claves privadas, que se asignan a las transacciones que realizan. Estas claves privadas actúan como firmas digitales personales. El creador del bloque o la persona que ejecuta la transacción ingresa la clave privada para la transacción, que encripta los datos de la transacción. Otros afectados por la transacción o aquellos que quieran acceder a los datos de la transacción pueden usar la clave pública del remitente para descifrarlos. Si hay algún cambio en el registro, la firma se volverá ilegal y la red de colegas descubrirá que se han realizado ciertas manipulaciones. La notificación temprana es esencial para evitar daños mayores, lo que hace que el sistema sea bastante seguro. El concepto de descentralización hace que la cadena de bloques sea más eficiente y segura. (Sharmaa & Prof. B. Balamurugan, 2020)

2.22 Descentralización en cadena de bloques

Blockchain es una red descentralizada, lo que significa que una persona o grupo no puede tener la autoridad de toda la red. No existe un sistema centralizado para controlar la gestión de la red blockchain. Cada nodo de la red tiene una copia del libro de cuentas, pero ningún nodo tiene derecho a cambiar el libro de cuentas. Para ejecutar cualquier transacción y cambiar el registro, todos los demás nodos de la red deben llegar a un consenso. Esta característica permite una red más segura.

Blockchain utiliza un modelo peer-to-peer, que permite que dos participantes interactúen sin la participación de un tercero o intermediario. Utiliza un protocolo P2P, lo que significa que los participantes de la red tienen la misma copia de la transacción, lo que permite sanciones mediante mecanismos de consenso. No se deducirán interrupciones ni costos adicionales durante este proceso. Para realizar cualquier actividad en la red, todos los nodos registrados en la red deben llegar a un acuerdo. En una red centralizada, si los piratas informáticos atacan el libro mayor central o la base de datos, todo el sistema se dañará. Pero la red descentralizada resuelve un problema, como no tener un solo punto de almacenamiento, por lo que no será atacado por usuarios no autorizados. (Sharmaa & Prof. B. Balamurugan, 2020).

2.23 Transparencia en la cadena de bloques

Aunque la información personal en la cadena de bloques es privada para los usuarios, la tecnología en sí es casi una especie de tecnología de código abierto permite a los usuarios de la red blockchain cambiar el código a voluntad, hasta que se obtenga el consenso de la mayoría de los participantes en la red. Dado que miles de usuarios están conectados a la red blockchain, es poco probable que alguien pueda realizar cambios sin que se dé cuenta. (Sharmaa & Prof. B. Balamurugan, 2020)

2.24 La arquitectura de la tecnología blockchain es la siguiente:

Cada nodo participante está ubicado en una red distribuida que utiliza bases de datos transaccionales y descentralizadas, y la información se almacena en bloques, los cuales están vinculados por contraseñas para hacer que la información sea inmutable.

Cada nodo de red tiene su propia copia de información en el libro mayor, que es compartida e inmutable. Blockchain permite la existencia de activos totalmente digitales como divisas, acciones, valores, registros y otros que pueden controlarse mediante el código informático del contrato inteligente.

Gracias a la blockchain. La computadora que ejecuta el código es la propia cadena de bloques, es decir, no es una computadora especial que pueda ser pirateada, sino cientos de miles de computadoras sincronizadas garantizan que el contrato no se pueda modificar y se ejecutará de acuerdo con las instrucciones. El consenso matemático se convierte en no hay necesidad de intermediarios humanos de terceros o la confianza matemática de computadoras que no son de confianza. El código (informático) se está volviendo más regular que nunca. (Quiroga Cruz, Jorge; Cubillos Herrera, 2018)

2.24.1 Funcionamiento Blockchain

- ✓ Cada nodo de la red posee un par de claves

- ✓ Cada usuario genera una dirección, un identificador en el sistema

- ✓ Cuando un nodo se registra para una transacción, sucederá lo siguiente:
- Genera el contenido de la transacción, incluida su clave pública y dirección.
- Si la información implica una transferencia, lleve la dirección de destino.

- ✓ Utiliza la clave privada para firmar la transacción.

- ✓ Las transacciones se extienden a través de una red distribuida.

- ✓ Cada vez que un nodo recibe una transacción que nunca antes había recibido chequea:
- La autenticidad de la firma.
- La validez lógica de la transacción. Si la verificación es correcta, se propagará al resto de nodos

- ✓ Una vez recibida y verificada la transacción, se incluirá en el grupo de transacciones. Nodo para generar un nuevo bloque

- ✓ El bloque de resultados incluye:
- Voluminoso.
- El texto con la información de la transacción.

- ✓ Una vez generado el bloque, se propagará en la red descentralizada. A medida que se generen nuevos bloques, la estructura de estos bloques evitará que se modifique el contenido.

- ✓ Cuando una transacción se comparte a través de nodos, cada nodo debe aceptar el resultado o modificarlo, para lo cual realiza un proceso de consenso. (Quiroga Cruz, Jorge; Cubillos Herrera, 2018)

Estructura de bloque (Shuyun Sh, 2020)

- ✓ Versión del bloque: reglas de validación del bloque;

- ✓ Hash del bloque anterior: valor del hash del bloque anterior;

- ✓ Timestamp: la hora de creación del bloque actual;

- ✓ No-ce: un campo aleatorio de 4 bytes que los mineros ajustan para cada cálculo hash para resolver un rompecabezas de minería PoW

- ✓ Raíz del cuerpo: valor de la raíz del árbol de Merkle construido por transacciones en el cuerpo del bloque;
- ✓ Hash de destino: umbral de destino del valor de hash de un nuevo bloque válido.

- ✓ El hash del objetivo se utiliza para determinar la dificultad del PoW rompecabezas

2.25 Blockchain para la aplicación de los HER

Hoy en día, muchos hospitales y clínicas utilizan blockchain para almacenar de forma segura los registros médicos de los pacientes. Cuando se genera y se prueba la historia

clínica del paciente, se puede agregar a la red blockchain, lo que proporciona una garantía de seguridad perfecta para el paciente y asegura que la historia clínica no se modificará. Estos registros médicos personalizados se pueden cifrar y almacenar en la red blockchain con una clave privada, lo que permite que solo los usuarios verificados accedan a los registros médicos en momentos críticos, garantizando así la privacidad de los pacientes. (Sharmaa & Prof. B. Balamurugan, 2020)

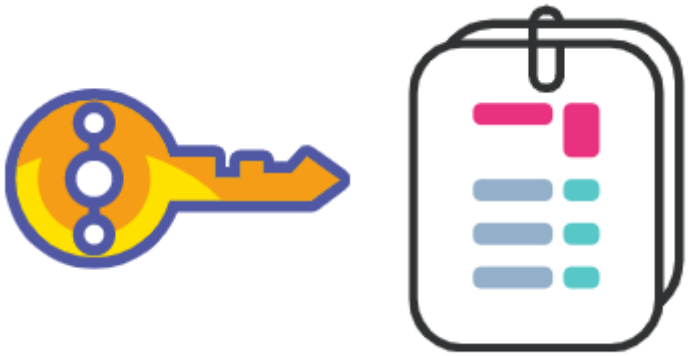


Figura 2.9 Lista de transacciones vinculada y asegurada

La interoperabilidad, la revisión de registros médicos en línea y la investigación juegan un papel vital en el futuro de la medicina. A través de blockchain, las personas, los proveedores de servicios y los investigadores médicos pueden compartir datos. Esta es la opinión de los investigadores de Mayo Clinic, una institución médica de los Estados Unidos: "Creemos que una red de datos basada en blockchain es una solución viable a este problema. El complejo tema de compartir datos de salud ".(Chari, 2020)

Registro público: Bajo el control y control del estado, actúa como una agencia de conexión entre ciudadanos y agentes del estado. A través de registros públicos, los ciudadanos pueden presentar solicitudes, escritos y comunicaciones a la administración pública. Además, a través de estos documentos también se registran los documentos enviados por los ciudadanos a entidades privadas o a las propias autoridades. La continua actualización de los documentos de ciudadanía refleja los cambios correspondientes y su trazabilidad, dando lugar así al concepto de "documentos de residencia". Un ejemplo de documento vivo es la "identidad digital soberana", el propósito de crear un sistema de identidad en línea es asociar datos con individuos. Los usuarios pueden controlar sus propios datos, es decir, se convierten en el verdadero propietario de los datos, y pueden elegir a quién se facilitan los datos, y a quién revoca los derechos de acceso. (Valiente, 2018)

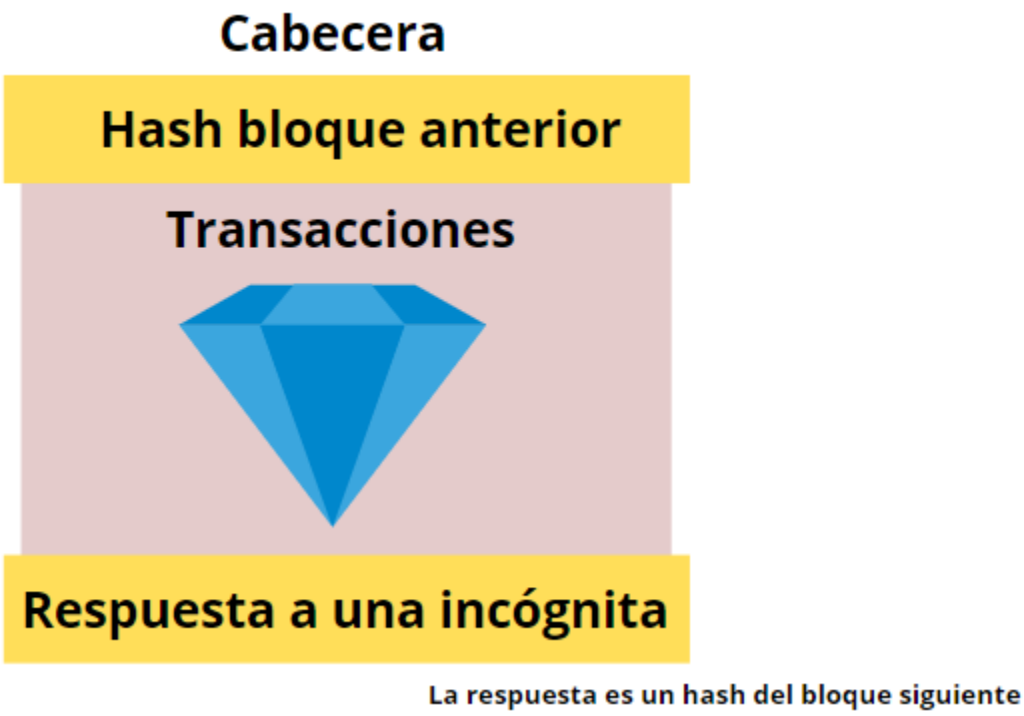


Figura 2.10 Estructura general de boque.

¿Cuáles son las ventajas que tiene deparado el uso de BlockChain en el sector salud? Recientemente, IBM informó que el 16 % de los ejecutivos de empresas en salud a las que les ofrecen servicios tenían planes sólidos para implementar una solución de BlockChain comercial en 2017, mientras que el 56 % esperaba comenzar en 2020. (Omar Gutiérrez, Jeffreys J. Saavedra, 2019)

2.25.1 Registros electrónicos de salud

El registro de salud electrónico (EHR) es un registro digital que recopila el historial médico del paciente. El registro médico electrónico se almacena electrónicamente en un formato digital y el hospital o el médico lo mantiene a lo largo del tiempo. El registro médico electrónico contiene todos los datos clínicos importantes esenciales para la atención del paciente y se almacena en un proveedor de atención específico, incluidos informes de resonancia magnética, exámenes médicos previos, inmunizaciones, informes de laboratorio y cualquier forma de alergia del paciente.

Estos registros son registros específicos del paciente en tiempo real, pueden ser utilizados cómodamente por pacientes o médicos y solo están disponibles para usuarios autorizados.

Puede compartir con ellos, otros proveedores de atención médica realizan mejores investigaciones en el campo médico a través de más de una organización de atención médica. Se mejoró el método tradicional de almacenar registros médicos de pacientes en papel, que es vulnerable a los ataques de muchas personas.

Amenazas como desastres naturales, robo, guerra, manipulación no autorizada, etc. Con EHR, puede acceder a la información automáticamente, es posible optimizar el flujo de trabajo de los médicos. También puede apoyar otras actividades relacionadas con la enfermería. Directa o indirectamente a través de varias interfaces. (Sharmaa & Prof. B. Balamurugan, 2020)

Estas experiencias están diseñadas para resolver preguntas actuales sobre cómo obtener historias clínicas de pacientes que han recibido diferentes tratamientos, su actualización en contexto dispersar y / o cruzar fronteras. La historia clínica se convertirá en "documentos múltiples distribuido ", agregara información almacenada en el centro donde fueron creados los registros médicos, archivados y actualizados dispersos por Hash y enlaces en forma de blockchain a paciente. (García-Morales, 2018)

La historia clínica electrónica contiene principalmente el historial médico del paciente, información estadística personal (como edad y peso), resultados de pruebas de laboratorio, etc. Por lo tanto, es importante garantizar la seguridad y privacidad de estos datos. Además, los hospitales de Estados Unidos y otros países / regiones también están sujetos a una supervisión estricta. En la práctica, el despliegue y la aplicación de sistemas de salud también enfrentan muchos desafíos.

Por ejemplo, como se mencionó anteriormente, el modelo de servidor centralizado es vulnerable a ataques de un solo punto y ataques internos maliciosos. Los usuarios que subcontratan o almacenan datos en estos sistemas de HCE (como los pacientes) a menudo pierden el control de sus datos y no tienen forma de saber quién accede a sus datos y con qué propósito (es decir, una violación de la privacidad personal). En este caso, la portabilidad y responsabilidad del seguro médico (HIPAA) establecido y firmado por el Congreso de EE. UU. 1996. Desarrolló políticas para mantener la privacidad y seguridad de la información médica personal y formuló varios procedimientos para controlar el fraude y el abuso en el sistema de salud.

Existe otro marco general para las pistas de auditoría de EHR, llamado ISO 27789, que se utiliza para permitir que la información de salud personal sea auditada entre sistemas y dominios. Siempre que se active una operación a través de un sistema que cumpla con la norma ISO 27789, se debe crear una pista de auditoría segura. Por lo tanto, hemos aumentado la importancia de un sistema de intercambio de datos colaborativo y transparente que también ayude con la auditoría y si se sospecha de mala conducta o Violación de datos, luego realice una investigación posterior al evento o una investigación

forense. Los investigadores forenses también enfatizaron este concepto (desde el diseño forense).

Como respuesta normativa a las preocupaciones de seguridad sobre la gestión de la distribución, el almacenamiento y la recuperación de los historiales médicos por la industria médica, impone requisitos a los sistemas médicos, incluidas medidas como la codificación de documentos y el uso de normas de firma digital para garantizar la autenticidad, la integridad y la confidencialidad de los historiales. (Shuyun Sh, 2020)

2.26 Auditoría de datos

El sistema de salud también se basa en la gestión de pistas de auditoría como mecanismo de seguridad, ya que ciertas excepciones pueden ser el resultado de un uso indebido o deshonesto de los derechos de acceso por parte de terceros o solicitantes de información. En caso de disputa, la pista de auditoría se puede utilizar como prueba para hacer que los usuarios sean responsables de su interacción con el registro médico. El libro mayor público inmutable y el contrato inteligente en la cadena de bloques pueden proporcionar un registro inmutable para todas las solicitudes de acceso para lograr la trazabilidad y la responsabilidad. El registro de auditoría contiene principalmente información importante y fácil de entender:

- Fecha y hora del evento registrado
- La identificación del usuario que solicita los datos
- Identificación del propietario de los datos a los que se accede
- Tipo de acción (crear, consultar, actualizar)
- El resultado de la validación de la solicitud

2.26.1 ¿nuevas características?

Blockchain es fundamentalmente un nuevo tipo de organización y la confianza que genera es muy diferente del concepto tradicional de confianza. Una variación de la creación de cadenas.
Las cadenas de bloques son diferentes en cuatro aspectos importantes. Las visiones teóricas tradicionales no pueden explicar estas diferencias. Estas diferencias crean un nuevo paradigma que se puede refinar y teorizar aún más:
En primer lugar, la creación de una cadena de bloques cambia fundamentalmente el enfoque de la organización y el sistema legal a uno en gran parte algorítmico, y extiende y mantiene la capa social relevante en la cadena de bloques. Ésta es la razón de los diferentes niveles de análisis. (Chawla, 2020)
“La cadena de bloques o blockchain sirve para gestionar datos y activos digitales” (García-Morales, 2018).

2.26.2 Normas y reglamentos

Si una nueva tecnología ingresa al mercado sin verificación de antecedentes, debe usarse con precaución, por ejemplo, basándose en un análisis de costo-beneficio. Por lo tanto, para mejorar el cumplimiento, la seguridad, la interoperabilidad y otros factores, necesitamos formular estándares, políticas y regulaciones unificadas (por ejemplo, estándares, políticas y regulaciones relacionadas con la seguridad y privacidad de los datos y el ecosistema blockchain). Por ejemplo, es posible que necesitemos diferentes mecanismos independientes y confiables para evaluar diferentes soluciones de blockchain para diferentes aplicaciones y contextos en términos de privacidad, seguridad, rendimiento, latencia, capacidad, etc. También debemos poder monitorear y hacer cumplir las sanciones por mal comportamiento y / o violaciones (por ejemplo, incumplimiento del contenido contractual). La cadena de bloques sufre de computación cara, gran almacenamiento y la gran anchura de banda en la parte superior puede no ser adecuada para la práctica y desarrollo de aplicaciones. Cuando muchas organizaciones participan en la red, el gran volumen de datos, las solicitudes frecuentes y la estabilidad de la cadena de bloques no puede ser ignorada. (Shuyun Sh, 2020)

2.26.3 Amenazas a la seguridad de las cadenas de bloques

Con el desarrollo de la tecnología blockchain, han aparecido varios ataques. Estos ataques o riesgos pueden ser causados por entidades o partes externas. La creciente popularidad de blockchain ha traído nuevos requisitos para proteger la privacidad y seguridad de la transmisión y el almacenamiento de datos. Las amenazas de seguridad de blockchain de hoy se pueden dividir aproximadamente en cuatro categorías: amenazas de doble gasto, amenazas cibernéticas, amenazas de grupos de minería y amenazas de seguridad de billetera. La siguiente sección explorará estas categorías, sus vectores de ataque, razones y contramedidas recomendadas. (Bhushan et al., 2020)

"La privacidad y confidencialidad, junto con la seguridad, son puntos clave que deberán asegurarse. En el estado actual las cadenas de bloques son imborrables lo que puede crear conflictos con aspectos como el derecho al olvido" (García-Morales, 2018)

2.27 La exactitud e integridad de los datos

(por ejemplo, no se permite la modificación no autorizada de los datos, que puede detectarse);

- ✓ Seguridad y privacidad de datos;
- ✓ Mecanismo de intercambio de datos eficiente
- ✓ Mecanismos para devolver el control de los registros médicos electrónicos a los pacientes (por ejemplo, los pacientes pueden monitorear su registro y recibir notificaciones de recolección o pérdida no autorizada);
- ✓ Revisión de datos y rendición de cuentas

Puede usar la cadena de bloques para lograr las propiedades anteriores, como se describe a continuación

- ✓ Descentralización. En comparación con el modelo centralizado, la cadena de bloques ya no necesita depender de la fianza de terceros.
- ✓ La seguridad. Puede resistir puntos únicos de falla y ataques internos en sistemas basados en blockchains distribuidos.
- ✓ Alias. Cada nodo está vinculado con un seudónimo público para proteger su verdadera identidad.
- ✓ Inmutabilidad. Es computacionalmente difícil de borrar o modificar cualquier registro de cualquier bloque contenido en la cadena de bloques unidireccional, función hash criptográfica.
- ✓ Autonomía. Los pacientes tienen derecho a poseer y compartir sus datos al configurar elementos especiales en el contrato inteligente, puede procesar sus datos de manera flexible.
- ✓ Incentivos. El mecanismo de incentivos de la cadena de bloques puede estimular la cooperación y la comunicación de instituciones competidoras y promover el desarrollo de servicios médicos e investigación.
- ✓ Auditable. Rastree fácilmente cualquier operación las transacciones históricas se registran en la cadena de bloques. (Shuyun Sh, 2020)

Por lo tanto, si la cadena de bloques se aplica correctamente al sistema EHR, puede ayudar a garantizar la seguridad del sistema EHR, mejorar la integridad, la privacidad de los datos, alentar a las organizaciones y a las personas a compartir datos además de promover la auditoría y la rendición de cuentas.

Sistema de registro médico electrónico basado en blockchain los requisitos de la nueva versión del sistema de registro médico electrónico seguro y las características del blockchain discutidas anteriormente, ahora describiremos los objetivos clave de implementar un sistema seguro de registro médico electrónico basado en blockchain. como sigue:

- ✓ Privacidad: los datos personales se utilizarán de forma privada y solo las partes autorizadas pueden acceder a los datos solicitados.
- ✓ Seguridad: Desde la perspectiva de la confidencialidad, integridad y disponibilidad (CIA):

- ✓ Confidencialidad: sólo los usuarios autorizados pueden acceder a los datos.
- ✓ Integridad: Los datos deben ser precisos durante la transmisión y las entidades no autorizadas no deben cambiarlos.

- ✓ Disponibilidad: No negará excesivamente a los usuarios legítimos el acceso a la información y los recursos.
- ✓ Auditabilidad: una parte importante de la seguridad. Por ejemplo, el registro de auditoría incluye principalmente información sobre quién accedió a qué EHR, con qué propósito y la marca de tiempo de cualquier operación a lo largo del ciclo de vida.
- ✓ Responsabilidad: Se auditarán personas u organizaciones y ser responsable de la mala conducta.
- ✓ Autenticidad: la capacidad de verificar la identidad del solicitante antes de permitir el acceso a datos sensibles.
- ✓ Anónimo: la entidad no tiene un identificador de privacidad visible.

Para lograr los objetivos anteriores, la investigación de salud existente basada en blockchain incluye los siguientes aspectos principales:

- almacenamiento de datos. Blockchain es una base de datos confiable que se utiliza para almacenar varios datos de salud privados. Al implementar el almacenamiento seguro, se debe garantizar la privacidad de los datos. Sin embargo, en la práctica, la cantidad de datos sanitarios suele ser grande y compleja. Por lo tanto, el desafío correspondiente es cómo lidiar con el almacenamiento de big data sin afectar negativamente el rendimiento de la red blockchain.
- Compartir datos. En la mayoría de los sistemas de salud existentes, los proveedores de servicios suelen mantener la gestión de datos primarios. Con el concepto de auto-soberanía, tiende a devolver la propiedad de los datos de salud a los usuarios que pueden compartir (o no compartir) sus datos personales a voluntad. También existe la necesidad de un intercambio de datos seguro entre diferentes organizaciones y dominios.
- Revisión de datos. En el caso de una disputa, el registro de auditoría se puede utilizar como evidencia para responsabilizar al solicitante de la interacción con el HCE. Algunos sistemas utilizan blockchain y contratos inteligentes para mantener la trazabilidad para la auditoría. Cualquier operación o solicitud se registrará en el libro de blockchain y se podrá recuperar en cualquier momento.
- Gestor de identidad. Es necesario asegurar la legitimidad de la identidad de cada usuario en el sistema. En otras palabras, sólo los usuarios legítimos pueden realizar solicitudes relevantes para garantizar la seguridad del sistema y prevenir ataques maliciosos. (Shuyun Sh, 2020)

Si existe un trabajo conjunto entre el gobierno colombiano y entidades públicas y privadas para ganar el impulso necesario para desarrollar proyectos enfocados a operaciones blockchain en diferentes organizaciones en Colombia. (Chari, 2020).

2.27 Python

Es un lenguaje de programación de múltiples paradigmas porque admite programación imperativa orientada a objetos y programación funcional. Es un lenguaje explicativo, dinámico y multiplataforma, ha sido gratis durante más de 20 años. Esta licencia pertenece a la licencia de Python Software Foundation, que es una organización sin fines de lucro que permite a las organizaciones y programadores modificar el código e implementar proyectos derivados, e incluso puede crear trabajos de código no abierto a partir de otros proyectos.

Este lenguaje de programación es ideal para el prototipo de blockchain por su popularidad en todo el mundo, por lo que se han creado miles de bibliotecas, módulos, códigos lo que representa una ventaja de implementación y desarrollo del algoritmo, Python además es una biblioteca de código fuente abierto para crear videojuegos y aplicaciones multimedia. Una de las librerías privilegiadas y precisas para la tecnología blockchain. Permite mostrar scripts geniales de una manera sencilla y entablar peticiones y respuestas entre el modelo cliente servidor por medio de los métodos http GET y POST, vitales para el desarrollo del prototipo de historias clínicas, el cliente y servidor están en constante dinámica de interacción, este además es conocido por su amplio abanico de posibles usos: desarrollo web, big data, inteligencia artificial, programación de videojuegos, finanzas, blockchain.

Le permite crear programas para diferentes plataformas y dispositivos. Adecuado para programas de escritorio Linux, Windows o Mac, además de permitir el desarrollo de diversas aplicaciones web e incluso juegos.

El desarrollo del código de programación basado en python comienza contextualizando los métodos GET y POST.

Para entender los métodos de GET y POST hay que entender que pasa cuando una persona interactúa con una página web.

El navegador puede enviar información al servidor de dos formas:

- Método HTTP GET. Información se envía de forma visible
- Método HTTP POST. Información se envía de forma no visible

2.28 HTTP REQUESTS – GET Y POST

Subimos un archivo a un POST, cuando pedimos información es GET. Ambos son requests, pero brindan servicios diferentes.

Interceptando HTTP REQUEST a través de un proxy se puede ver con una lupa la conversación entre navegador y cliente, dependiendo si la información va cifrada o no, el poder observar o modificar los request.

2.28.1 Método HTTP GET

El método GET envía directamente la información codificada del usuario en el encabezado de la solicitud HTTP en la URL. La página web y la información codificada se separan por un interrogante_ ?

- El método GET envía información en la propia URL y la longitud está limitada a 2000 caracteres.
- La información es visible, por lo que nunca utilizará este método para enviar información confidencial.
- No se pueden enviar datos binarios (archivo, imagen ...).
- En PHP, los datos se administran mediante una matriz asociativa $_ GET.

2.28.2 Método HTTP POST

Al usar el método HTTP POST, la información también se modificará, pero se enviará en el cuerpo de la solicitud HTTP, por lo que no aparecerá en la URL.

- El método POST no tiene límite en la cantidad de información que se enviará.
- La información proporcionada no es visible, por lo que se puede enviar información confidencial.
- Se puede utilizar para enviar tanto texto normal como datos binarios (archivos, imágenes).
- PHP proporciona una matriz asociativa $_ POST para acceder a la información enviada.

2.29 Protocolos para desplegar una blockchain válida e inmutable

Con los algoritmos de consenso, hashing, registro inmutable, red2p2, minado.

Dos métodos para implementar encriptación simétrica, BLOCK y STREAM

1. Block un tipo de clave simétrica que opera en un grupo de longitud fija

    - NIST (National institute of standards technology) es la entidad que modela la data encryption standard “DES”
    - Otro standard desarrollado fue Triple Data Encryption Standard”3DES”
    - Algoritmos Block CIpher comunes: IDE, RC2, RC5, SKIPJACK

2. Stream cifrado simétrico donde los dígitos del input son encriptados uno a la vez

- Son más rápidos que block y requieren menos complejidad de hardware

2.29.1 Encriptación asimétrica

Utiliza dos llaves separadas (pública y privada), una para cifrar otra para descifrar, ambas llaves son generadas al mismo tiempo y están relacionadas, la clave privada se mantiene secreta, la clave pública se distribuye al mundo.

2.30 Postman

Postman nace de una herramienta que principalmente permite crear solicitudes en la API de una forma muy sencilla y poder testear la API de esta forma. Todo basado en la extensión de Google Chrome. El usuario puede ser un desarrollador que está verificando las operaciones de la API que se van a desarrollar, o un operador que está realizando tareas de monitoreo en la API.

En torno a la idea de probar los algoritmos de blockchain, Postman proporciona un conjunto de utilidades adicionales que pueden administrar y validar las funciones preestablecidas en el código de la estructura de la cadena de bloques de una manera más sencilla y visual. Es por ello que proporcionará herramientas para registrar acciones dentro de la cadena, monitorear las funciones del algoritmo, crear validez del bloque, verificación de inmutabilidad, consenso y hashing. Postman una plataforma de desarrollo de API basada en el modelo de desarrollo.

2.31 Anaconda cloud

Anaconda es una suite de código abierto que contiene una serie de aplicaciones, bibliotecas y conceptos diseñados para el desarrollo de la ciencia de datos usando Python. Generalmente, la distribución de Anaconda es una distribución de Python que puede actuar como administrador de entorno, administrador de paquetes y tiene una colección de paquetes de código abierto.

La distribución de Anaconda se divide en 4 áreas o soluciones técnicas, Anaconda Navigator, Anaconda Project, Data Science Bookstores y Conda. Todos estos se pueden instalar automáticamente mediante un proceso muy simple.

Anaconda proporciona todas las herramientas técnicas de configuración para permitir un entorno de programación con el fin de desarrollar el código blockchain, derivando de su distribución el despliegue los algoritmos antes mencionados, se puede administrar a través de la interfaz gráfica de usuario Navigator, compilar, validar y operar. También mediante la consola usando Conda. Permite instalar, eliminar o actualizar cualquier paquete de anaconda con unos pocos clics en el navegador o con un solo comando de Conda.

2.30 Spyder

En el mercado, existen varios IDE que se pueden usar para desarrollar proyectos de aprendizaje automático como blockchain, la mayoría de los cuales son gratuitos, y cada desarrollador puede elegir el IDE que más le convenga.

Spyder es uno de los IDE utilizados para el propósito de desarrollo blockchain, permite desplegar los algoritmos requeridos para establecer un prototipo de cadena inmutable. Es de código abierto, escrito en Python y utilizado para el desarrollo de Python, con un enfoque en la investigación de tecnologías como cadenas de bloques, el análisis de datos y la creación de paquetes de software científico son fundamentales en tecnologías nuevas e innovadoras. Spyder proviene del acrónimo en inglés "Scientific PYthon Development EnviRonment" y tiene una interfaz de usuario bien diseñada con opciones interactivas, diseños personalizables y partes intercambiables.

Sus características incluyen un editor multilingüe con finalización automática de código en tiempo real y definiciones de referencia. También contiene registro de historial, herramientas de desarrollo, visor de documentos, explorador de variables y consola interactiva.

Algunas características clave de Spyder son las siguientes:

- Multiplataforma y se puede utilizar para Linux, Windows y macOS.
- Libre y de código abierto.
- Resaltado de sintaxis.
- Admite varios idiomas.
- Consola interactiva.
- Navegador variable.
- Visor de documentos, visualización de gráficos y datos
- Admite la expansión de funciones a través de complementos y API.

2.31 PyCharm

PyCharm es el IDE de Python y además cuenta con una versión apta para distribuciones Gnu / Linux, lo que facilita el uso y la creación de programas como blockchain con este lenguaje de programación. PyCharm es un IDE, es decir, no es solo un editor de código, también existen depuradores, intérpretes y otras herramientas que ayudan a crear y exportar los programas con el modelo cliente servidor detrás de blockchain que son creados basados en esta tecnología. PyCharm cuenta con un intérprete en el editor de código, que ayudará a entender o conocer posibles errores en el código en tiempo real, lo que hace que usuarios de la cadena de bloques interactúen con un sistema software más eficiente y simple. La

programación de Python a través de PyCharm es inteligente e integrable en sistemas de historiales clínicos a través del diseño del prototipo blockchain.

El uso de PyCharm tiene ventajas básicas relacionadas con el prototipo blockchain para historias clínicas (similares a las que ofrecen otros IDE), pero también tiene algunas ventajas específicas debido a su popularidad, practicidad y desarrollo evolutivo. Por lo tanto, PyCharm tiene un editor inteligente que le permite usar algunos atajos de librerías y bibliotecas de criptografía digital además de compatibilidad con otros algoritmos como autenticadores, verificadores de identidad, Etc. Para completar el código de manera lógica y relacional. Del mismo modo, nos permite navegar por el código y saltar entre las clases y métodos creados, lo que hace que el flujo de trabajo sea más dinámico.

Una de las características distintivas de PyCharm es la capacidad de refactorizar el código, lo que generalmente significa modificar el código sin comprometer su ejecución.

Permite la integración con otros lenguajes y frameworks (como Node JS) y facilita el acceso a la base de datos y la depuración.

En Python, se recomienda encarecidamente que utilice un marco con dependencias de paquetes independientes y un intérprete, llamado entorno virtual. El IDE ayuda a crear y mantener entornos virtuales de forma sencilla, permitiendo:

- Crea un entorno virtual para cada proyecto.
- Entorno virtual compartido.
- Cada intérprete de cada entorno puede ser una versión diferente de Python.
- Detecta cambios en el archivo requirements.txt del proyecto para instalar dependencias.
- Gestione los paquetes de Python de forma fácil e intuitiva.

2.32 Google Authenticator

Google Authenticator es una aplicación creada por Google para proporcionar códigos que puede usar para verificar su identidad después de ingresar su nombre de usuario y contraseña. Puede usarse para mejorar la seguridad de su cuenta de Google, pero es compatible con otros servicios. Esta es una aplicación simple, solo muestra un código numérico de seis dígitos, que cambia cada 30 segundos, y debe usarlo para verificar su identidad después de iniciar sesión.

La ventaja de usar un autenticador en una aplicación de blockchain es que permite validar la identidad del agente que busca interactuar dentro de la cadena, lo cual es sumamente importante en un sistema de salud, esta utilidad CLI se puede ejecutar en cualquier lugar

donde se pueda ejecutar Python 3.5 desde una interfaz de línea de comandos (por ejemplo, una ventana de terminal) y una base de datos de cuentas. Los secretos están restringidos por la plataforma y están protegidos por contraseña. La contraseña protegida cifra el archivo, y se puede realizar una copia de seguridad del archivo y copiarlo entre varios sistemas sin preocuparse de que los malos actores obtengan la autoridad de la autenticación del segundo factor.

El cliente TFA / MFA que genera el código digital "único" necesita una contraseña compartida con el servidor para verificar la verificación de identidad. Por lo general, este secreto es generado por el servidor y capturado por el cliente en forma de código QR o KEY, permitiendo al cliente sellar una apertura de interacción con los servicios del sistema blockchain.

Estado del arte

El capítulo de estado del arte es una especie de investigación bibliográfica, sobre las bases de investigación de diferentes autores estrechamente relacionados con la tecnología blockchain aplicada al sistema de salud, trata temas específicos. Buscar, leer y analizar bibliográficamente los contextos encontrando y relacionados con los temas deseados en el estudio de la blockchain orientado a la traza de historiales clínicos. Este ejercicio muestra lo que se ha hecho sobre un tema en particular, en qué medida ha llegado, qué tendencias han surgido, cómo ha surgido su producto, así como cuáles son los problemas de aplicabilidad y prueba de campo.

En el campo de la salud, la tecnología blockchain en Colombia e internacional ha sido una de las mejores opciones durante algún tiempo. En 2018, en Cundinamarca, Colombia, se desarrolló un modelo de red blockchain para evitar problemas causados por una formulación inadecuada de medicamentos y resolver el problema de los eventos adversos causados por los medicamentos. El sistema ha sido implementado en la red hospitalaria del departamento, y es el primero en utilizar esta tecnología para implementar el sistema a nivel nacional y obtener un alto reconocimiento. El sistema consta de una fuente de datos que brinda contraindicaciones para cada fármaco, una capa donde se ubican las reglas de negocio y una capa donde se expondrán los servicios web y estarán listos para ser utilizados por cualquier software que quiera aprovechar esta función.

El gobierno y los sectores industriales relacionados están cada vez más interesados en la digitalización del sistema de salud, lo cual está parcialmente probado en diversas iniciativas implementadas por diferentes países y departamentos.

De acuerdo con las consultas realizadas, es claro que a partir del artículo no aborda la gestión y posibles aplicaciones del sector salud colombiano para implementar el desarrollo blockchain; sin embargo, HCEU (Historia de la Medicina) Uni-Electronics) es el producto más cercano que se utiliza en Colombia.
En Cundinamarca, se está implementando un proyecto de historia clínica electrónica unificada (HCEU) Se trata de un proyecto de transformación tecnológica a gran escala que busca optimizar e integrar diferentes recursos de información de los servicios de salud departamentales mediante el uso de tecnologías de conectividad e interoperabilidad para crear una red de información departamental. El proyecto tiene como objetivo unificar las historias clínicas de 35 hospitales de la red pública departamental, incluidos sus departamentos funcionales centros y puestos de salud, la automatización de la información captada a través de las historias clínicas. En España se descubrió un proyecto denominado "pasaporte de empleado", que tiene como objetivo desarrollar una solución basada en la tecnología blockchain en la actual crisis sanitaria y social, que pueda introducir y consultar

con COVID -19 Probar datos médicos relacionados para determinar la identidad de los empleados.

BC-MED: Una plataforma de historia clínica electrónica basada en la tecnología blockchain. Actualmente, solo existe un sistema fragmentado, no estandarizado, no interconectado en el Departamento de Ingeniería del Sistema, Norte de Barranquilla Colombia, que restringe esta información de alguna manera. De puntos de acceso. En los últimos años, diversos mecanismos han tratado de hacer realidad la descentralización. Blockchain es un ejemplo, por su naturaleza participativa ha producido una tecnología que permitirá el uso de la información para construir sistemas sin depender de una sola instancia. (Omar Gutiérrez, Jeffreys J. Saavedra, 2019)

Por otro lado, en 2017, también se propuso una plataforma basada en blockchain denominada BC-MED para la gestión de historias clínicas aplicadas al sistema de salud colombiano, con el propósito de convertir el sistema centralizado que actualmente utilizan las instituciones de salud, el sistema es completamente interoperable para compartir información y mantener registros electrónicos únicos a los que los pacientes puedan acceder fácilmente. Por este motivo, el sistema está diseñado para permitir que los pacientes posean, controlen y compartan sus datos de salud de una manera fácil y segura sin infringir la privacidad, lo que proporciona una nueva forma potencial de mejorar la inteligencia del sistema médico. Los datos del paciente se mantienen en secreto. Modelo propuesto para tener derechos de acceso con fines de investigación para garantizar que los pacientes poseen y controlan sus datos de atención médica, revocando así la autorización a las instituciones médicas. (Mellizo Gomez & Minú Dussán, 2020)

Columbia Clinic es pionera en tecnología blockchain en América Latina la Clínica las Américas de Medellín está implementando el primer caso de aplicación de la tecnología blockchain al monitoreo, control y suministro de equipos médicos (como catéteres, marcapasos, etc.).

"Gracias a la implementación de esta solución de tecnología blockchain, pudimos reducir la entrega de consumibles a solo 24 horas, reducir el tiempo de facturación en un 90% y reducir los errores de órdenes de compra en un 60%", dijo el Dr. Juan Gabriel Cendales, gerente de Clínica Las Américas, presentó la primera aplicación de la tecnología en el sector salud del país.
Con esto, Clínica Las Américas, ubicada en Medellín, es pionera en América Latina en el uso de blockchain de IBM para lograr la trazabilidad de dispositivos médicos. Este avance se espera que se convierta en la base del sistema de salud de Colombia, ya que se estima que 9 millones de personas son hospitalizadas cada año en el país. (dinero, 2018)

A nivel internacional se han realizado algunos estudios, como el realizado en 2016 por la Clínica Mayo, una de las clínicas más importantes de Estados Unidos, que definió un

sistema para compartir información médica entre sus instalaciones. Sí, utilizan La red Blockchain, en comparación con otras clínicas que administran el sistema local, esta red tiene una gran ventaja en la consulta médica. El blockchain implementado en este trabajo se basa en una red pública distribuida, y el mecanismo de consenso implementado en la misma investigación se agrega a la red para asegurar. Sin embargo, la red pública de blockchain ante la necesidad de utilizar un algoritmo de consenso complejo para registrar nuevas transacciones en la red, se enfrentan a un gran problema de velocidad de acceso a la información, que tiene grandes desventajas en comparación con las blockchains privadas. Distribuido y almacenado de forma segura en toda la red. (Mellizo Gomez & Minú Dussán, 2020)

Por otro lado, en los Estados Unidos, el MIT ha desarrollado un sistema de gestión de registros descentralizado que utiliza tecnología blockchain para procesar registros médicos, llamado MedRed. El sistema proporciona a los pacientes registros completos e invariables de fácil acceso a sus Información médica de todos los proveedores y lugares de tratamiento. Al aprovechar los atributos únicos de blockchain, MedRec puede administrar la verificación de identidad, la confidencialidad, la responsabilidad y el intercambio de datos. Consideraciones importantes al manejar información confidencial. El diseño modular está integrado con las soluciones de almacenamiento de datos locales existentes del proveedor, lo que promueve la interoperabilidad y si el sistema es conveniente y flexible. Por lo tanto, MedRec permite el surgimiento de la economía de datos, proporcionando grandes datos para empoderar a los investigadores al tiempo que involucra a los pacientes y proveedores en la elección de liberar metadatos. Sin embargo, esta solución no considera una historia donde se tenga en cuenta los determinantes familiares, económicos y sociales que puedan afectar la salud de un paciente. (Mellizo Gomez & Minú Dussán, 2020)

Otra importante contribución a la gestión de registros médicos es MeDShare, en el que propusieron un sistema que resuelve el problema del intercambio de datos médicos entre los custodios de grandes bases de datos clínicas en un entorno de poca confianza. El sistema se basa en blockchain y proporciona Información de datos, auditoría y control compartido entre entidades de big data en la nube. MeDShare supervisa las entidades que acceden a los datos de los sistemas de alojamiento para detectar un uso malintencionado. En este modelo, la conversión e intercambio de datos de una entidad a otra entidad y todas las operaciones realizadas en el sistema se registran a prueba de manipulaciones, y el sistema utiliza contratos inteligentes y acceso a mecanismos de control para rastrear de manera efectiva el comportamiento de los datos y cuando se detecta un conflicto de permisos de datos, se revoca el acceso a la entidad problemática. (Mellizo Gomez & Minú Dussán, 2020)

El marco Hyperledger Fabric y la tecnología blockchain se han utilizado para diseñar modelos centrados en el paciente para intercambiar registros médicos. Por ejemplo, en 2017, la organización de la cadena médica propuso un sistema para la gestión de registros

médicos electrónicos, que hace que los registros médicos sean únicos y descentralizados, y permite a los pacientes controlar sus registros médicos, lo que les permite comunicarse con su red médica. Cada organización comparte la versión más completa del registro.

La relación del estado del arte se expresa en la siguiente tabla 1

Autor(es)	Título	Tomado	Año	Aporte
Bharat Bhushan, Preeti Sinha, Andrew J	Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions	ScienceDirect	2020	Bases teóricas de blockchain orientadas a la salud. Criptografía, hash, consenso..
Chetan Chawla	Trust in blockchains: Algorithmic and organizational	ScienceDirect	2020	Bases teóricas de blockchain orientadas a la salud. Confianza en blockchains,Limitaciones de blockchains
Cristian Alejandro Chisaba Pereira	La gestión en salud a través del blockchain: una herramienta del futuro inmediato	https://revistas.unbosque.edu.co	2017	Bases teóricas de blockchain orientadas a la salud. La tecnología blockchain como estrategia en la gestión de la salud, Sus bondades y posibilidades
Davinson Mellizo Gomez, Juan Minú Dussán	Modelo basado en Blockchain para la implementación de una historia clínica electrónica familiar	RITI, SEICIT	2020	Bases teóricas de blockchain orientadas a la salud. Blockchain privada Vs Blockchain pública, Arquitectura, Roles del sistema
Massimo Di Pierro	What Is the Blockchain?	Computing in Science & Engineering	2017	Bases teóricas de blockchain orientadas a la salud. Hash Functions, Cryptocurrencies and Beyond
García-Morales, Elisa	Luces y sombras sobre el impacto del blockchain en la gestión de documentos	f. tecnologías de información, normativa y gestión de la información	2018	Bases teóricas de blockchain orientadas a la salud. Se inicia la siguiente revolución en internet, Historias clínicas, Firma

				electrónica y certificación de documentos
Javier Leyton	Health Chain lanza red basada en blockchain para unificar la historia clínica de los pacientes en América Latina	IBM cloud	2020	Bases teóricas de blockchain orientadas a la salud. Beneficio logrado
Jorge Alejandro Quiroga Cruz & Sergio David Cubillos Herrera	Fundamentación de un modelo mediante la tecnología blockchain para el tratamiento de información en el área de vigilancia epidemiológica de la clínica Juan N. Corpas.	Universidad Distrital Francisco José de caldas Facultad de Ingeniería Especialización en Ingeniería de Software	2020	Bases teóricas de blockchain orientadas a la salud. fundamentación, alcance, conceptos generales
Jhony Salazar Martínez	Acercamiento a la tecnología Blockchain y posibles aplicaciones en el sector salud en Colombia	Revista CIES	2020	Bases teóricas de blockchain orientadas a la salud. Bitcoin, los inicios de Blockchain, Cómo está formada la Blockchain, que ofrece Blockchain.
Oscar fernando velasquez viancha	Ventajas del desarrollo e implementación de blockchain en empresas públicas y privadas de colombia	Universidad santiago de cali	2020	Bases teóricas de blockchain orientadas a la salud. Origen del Blockchain, Bitcoin, Ethereum, Propiedades fundamentales de la cadena de bloques
David Lizcano	Blockchain: posibilidades y aplicaciones al dominio de la medicina y los datos clínicos	MOL2NET, International Conference Series on Multidisciplinary Sciences	2018	Bases teóricas de blockchain orientadas a la salud. el Blockchain, para revolucionar la gestión digital de datos de historial clínico, de diagnósticos y consultas a expertos y especialistas
Rubal Jeet, Sandeep Singh Kang	Investigating the progress of human e-healthcare systems with	ScienceDirect	2020	Bases teóricas de blockchain orientadas a la salud. Background, Blockchain, Alternative

	understanding the necessity of using emerging blockchain technology			Crypto-Currencies and blockchains
Iman Ghasemian Sahebi	Expert oriented approach for analyzing the blockchain adoption barriers in humanitarian supply chain	ScienceDirect	2020	Bases teóricas de blockchain orientadas a la salud. Blockchain technology, Blockchain adoption barriers
Muneeb Ul Hassan a,	Differential privacy in blockchain technology: A futuristic approach	ScienceDirect	2020	Bases teóricas de blockchain orientadas a la salud. Privacy of blockchain, Consensus and mining in blockchain
Prateek Pandey, Ratnesh Litoriya	implementing healthcare services on a large scale: Challenges and remedies based on blockchain technology	ScienceDirect	2020	Bases teóricas de blockchain orientado a la salud.Tecnología blockchain, Tipos de blockchain
Yogesh K. Dwivedi	Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life	ScienceDirect	2020	Bases teóricas de blockchain orientadas a la salud. Información imperfecta, Transformación en la industria de la cadena de suministro
Zhi Li, Ali Vatankhah Barenji	Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform	ScienceDirect	2018	Bases teóricas de blockchain orientadas a la salud. Blockchain, Consortium BC, Public BC Private BC
Niclas Kullig, Philipp Lämmel	Prototype Implementation and Evaluation of a Blockchain Component on IoT Devices	ScienceDirect	2020	Bases teóricas de blockchain orientadas a la salud. Blockchain, arquitectura, Implementation, Blockchain based Smart Contracts, Configuration

Shubhani Aggarwal ,Neeraj Kumar	Blockchain 2.0: Smart contracts	Advances in Computers	2020	Bases teóricas de blockchain orientadas a la salud. Contratos inteligentes utilizados en un sistema descentralizado, Plataformas blockchain que utilizan transacciones
Xiang FU, Huaimin WANG	A survey of Blockchain consensus algorithms: mechanism, design and applications	SCIENCE CHINA	2019	Bases teóricas de blockchain orientadas a la salud. Problema de los generales bizantinos y algoritmos de consenso de Blockchain, Modelo de proceso de algoritmo de consenso de blockchain, Confirmación de transacción

Tabla 1. Estado del arte

Métodos de investigación

Los métodos de investigación son procedimientos estrictos que los investigadores deben seguir al adquirir conocimientos y están formulados de manera lógica. Estos métodos consisten en una serie de procesos que los humanos deben tomar al investigar y probar la verdad.
Este capítulo se refiere a un procedimiento que se puede seguir para probar hipótesis, alcanzar metas o dar respuestas específicas a preguntas descubiertas en el mundo de las tecnologías emergentes más precisamente blockchain, parte de la definición de las redes de tipología distribuida y lo primero que hay que observar es qué instancia cubre. Si comienza con situaciones específicas y desea encontrar información sobre ellas y analizarlas utilizando un marco teórico general, entonces se referirá a la inducción. Si comienza con situaciones generales explicadas por marcos teóricos generales y tiene la intención de aplicarlas a realidades específicas (sus objetos de investigación), entonces utilizará inferencias. Lo importante es que sepa de dónde proviene el conocimiento y adónde espera llegar. El método que desea seguir en la propuesta siempre debe hacerse con referencia a la pregunta planteada.

4.1 Diseño metodológico

La investigación es un conjunto de métodos utilizados para obtener una comprensión profunda de un problema o generar nuevos conocimientos en un campo de aplicación. Las características de todo lo relacionado con blockchain o tecnología blockchain para enfocar y comprender claramente su organismos públicos y privados en Colombia. Es una herramienta importante para el progreso científico porque permite verificar o descartar hipótesis con parámetros confiables, de manera sostenida en el tiempo y con metas claras. Esto asegura que las contribuciones al campo del conocimiento de la investigación puedan ser verificadas y replicadas.

4.2 Tipo de investigación

Investigación aplicada, el objetivo es encontrar estrategias que se puedan utilizar para resolver problemas específicos. La investigación aplicada utiliza la teoría para generar conocimientos prácticos, y es muy común en ramas del conocimiento como la ingeniería o la medicina. Investigación tecnológica aplicada, ayuda a generar conocimiento que puede ser utilizado en el sector productivo para promover un impacto positivo en la vida diaria.

4.3 Fuentes y técnicas de recolección de información

Los recursos utilizados para la investigación son secundarios, los artículos e investigaciones anteriores están todos orientados a los temas de blockchain, sus características, atributos y aplicaciones para decidir si desarrollar e implementar blockchain en la organización. Las técnicas de recopilación de información se llevan a cabo mediante el análisis de la literatura utilizando como fuentes artículos científicos alojados en la web.

Actividades
· Búsqueda de información requerida y delimitación de referencias de acuerdo al material académico disponible en los artículos de la web.
· Detalle de las características de la cadena de bloques para tener una perspectiva clara y concisa del por qué implementarla en las organizaciones.
· Descripción de los tipos de Blockchain y las aplicaciones en las diferentes áreas.
· Descripción de los algoritmos y estándar detallando las características fundamentales al momento de usarla por medio de la cadena de bloques.

4.4 Fases de desarrollo

El ciclo de vida del proyecto historias clínicas basadas en tecnología blockchain se estructura en cinco etapas: inicio, planificación, ejecución, seguimiento y finalización. En este capítulo, se explicará la composición de cada fase, basando los resultados en los objetivos específicos y generales, las actividades, mecanismos de investigación y adquisición de datos congruentes estrechamente relacionados con la tecnología blockchain orientada a las transacciones de historias clínicas.

4.4.1 Inicio
La fase inicial es fundamental para el ciclo de vida del proyecto, porque es el momento de definir el alcance y estructurar la aplicabilidad de las historias clínicas basadas en tecnologías de redes descentralizadas. Solo cuando el alcance y la pregunta del problema están seriamente estructuradas, representa un verdadero valor y punto de partida a nivel general dentro del proyecto, si están claramente definidos los objetivos y propósitos se puede garantizar el éxito. Este es también el momento de compartir la visión con las partes interesadas en la cadena de bloques para un sistema de salud regional, proyectado a lo global y buscar un compromiso y apoyo en cada agente de la tecnología.

4.4.2 Planificación
Esta es considerada la etapa más difícil de la implementación de tecnología de tipo distribuida, porque tiene que resolver las dudas y orientar el desarrollo del prototipo basado en algoritmos de encriptación y validez de los agentes de la cadena, calcular la demanda de lenguaje de programación, la operatividad del sistema y los altos flujos de data que

atraviesan los nodos dentro de la cadena ,como también los recursos y equipos que deben establecerse plenamente dentro de un sistema blockchain. Requerimientos que esperan poder lograr los objetivos a tiempo dentro del rango de parámetros. Además, también debe planificar las actividades de prueba y calibración del prototipo, los contratos y las comunicaciones. En última instancia, se trata de crear un plan de proyecto completo y establecer una hoja de ruta clara.

4.4.3 Ejecución

Según el plan, es necesario completar las actividades y tareas planificadas para el desarrollo del prototipo blockchain, continuar con la entrega de productos intermedios y garantías de la funcionalidad del proyecto. Es importante garantizar una buena etapa de ejecución con el fin de dar garantía de una mejora en control del progreso y los plazos. Asimismo, se debe monitorear la evolución de la tecnología de manera local, el consumo de recursos de la plataforma en desarrollo, presupuesto y tiempo, para ello suele ser necesario contar con herramientas de gestión de proyectos de investigación. Esta etapa debe administrar: riesgos de la tecnología blockchain, cambios dentro del prototipo, eventos adicionados al desarrollo, requerimientos, recursos de las redes distribuidas, tiempo, actualizaciones y modificaciones dentro del diseño de la cadena de bloques.

4.4.4 Seguimiento y control

Esta etapa incluye los procesos necesarios para dar seguimiento, revisar y monitorear el avance del proyecto. Se considera un medio para detectar desviaciones lo más rápido posible con el fin de identificar áreas donde el plan puede necesitar ser cambiado. La fase de seguimiento y control está naturalmente asociada a la fase de ejecución, aunque por su importancia y valor clave no puede concebirse desde la fase de ejecución únicamente.

4.4.5 Cierre

Esta etapa incluye todos los procesos destinados a la finalización formal del proyecto y las obligaciones contractuales inherentes. Los resultados son básicamente el núcleo de la etapa final, en ellos se evidencia el éxito que tomó el proyecto con bases sólidas medible por la garantía de la implementación del prototipo de registros médicos. Una vez finalizada esta etapa, se determina oficialmente que el proyecto ha finalizado.

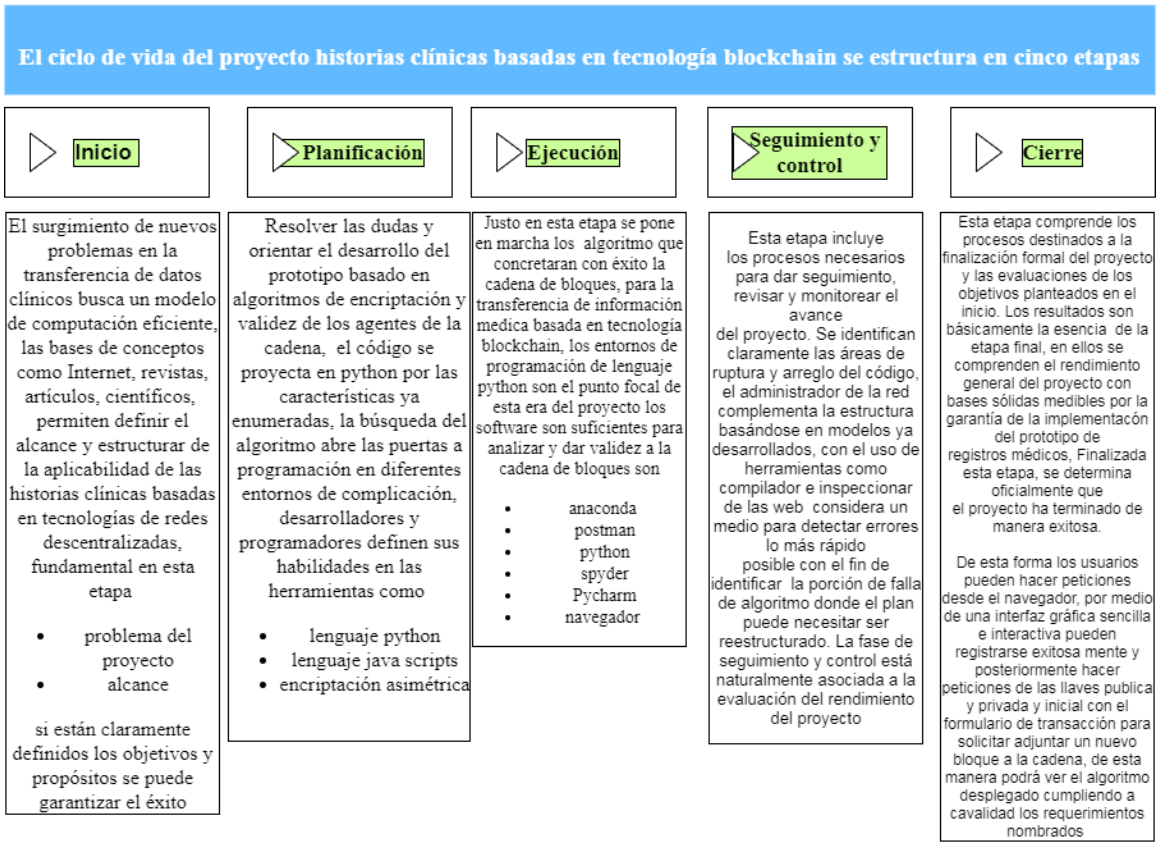


Figura 4.1 Etapas de desarrollo

Desarrollo del prototipo basado en Python

Este capítulo da una vista previa del prototipo basado en Python, cómo funciona la red tipo distribuida, desarrollo del código, relación entre herramientas y entornos e interacción de usuarios. Se expone de manera clara cada etapa en la puesta en marcha del prototipo, así como el contexto de programación en sus múltiples paradigmas en la operatividad de aplicaciones mediante tecnología blockchain, Python es ideal para el prototipo de blockchain por su relación con la criptografía y encriptación asimétrica en el mundo digital, el código representa la implementación y desarrollo del algoritmo.

Permite mostrar scripts de una manera intuitiva, sencilla y confiable para entablar un modelo de peticiones y respuestas entre el cliente y el servidor, por medio de los métodos http GET y POST. Cada agente de la cadena es vital para el cumplimiento del modelo de historias clínicas basado en blockchain, Python será quien, dé soporte a este prototipo de manera adyacente e intuitiva. Paciente y médico estarán en constante dinámica de interacción, este además es un modelo amplio en el repertorio de algoritmos a seguir por su amplio abanico de posibles usos blockchain.

Para tener un concepto más claro, los requerimientos del prototipo son requisitos, acciones o parámetros mínimos para que la propuesta entre en una etapa de marcha y desarrollo. Es decir, se trata de una solicitud que hace cada característica del algoritmo para desplegar la blockchain en las transacciones de historiales clínicos, de manera segura que permita a usuarios y servidores entablar una sintaxis coherente y calificada para atender sus necesidades de agregar, transferir y consultar los datos en el libro mayor contable “BLOCKCHAIN”. Todas las tecnologías utilizan requisitos para satisfacer sus necesidades con el fin de lograr su propósito de manera exitosa.

Como mencionamos de validación y verificación de la tecnología emergente, un requisito donde se empleen los términos y se determine los algoritmos de codificación mínimos para que la red blockchain este pertinentemente valorada y validada dentro del contexto de estudio en las historias clínicas en la solicitud se identifican los algoritmos de tecnología distribuida. Discutir los términos de referencia del blockchain, las especificaciones algorítmicas de la app distribuida al igual que la documentación tecnológica e innovadora del proyecto.

5.1 Para desarrollar el código

Primero se instala flask que es un framework, permite crear una página web donde se va contener la blockchain, Flask es un marco minimalista escrito en Python que le permite crear rápidamente aplicaciones web con un mínimo de líneas de código. Se basa en la especificación WSGI de Werkzeug y el motor de plantillas Jinja2, y tiene licencia BSD.

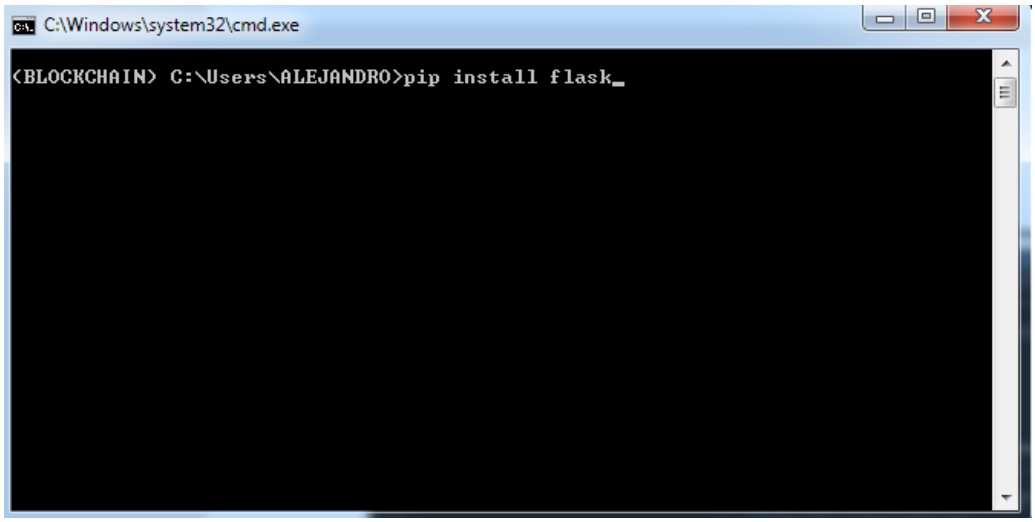


Figura 5.1 Comando instalar flask

5.2 Blockchain en 2 pasos

5.2.1 Se arma blockchain

Figura 5.2 se importan los paquetes que definirán la estructura arquitectónica de blockchain, paquetes como (datetime, hashlib, json, flask, jsonify) que permiten darle identidad al bloque crear web app, codificar los hashes, cada uno de estos con relación a la validez de los bloques

```
#Blockchain
#Armando la blockchain

import datetime #cada bloque tiene su datetime el dia  hora exacto
import hashlib #hashar los bloques
import json #codificar los bloques antes de hasharlos
from flask import flask, jsonify #crear web app
```

Figura 5.2 Importando los paquetes que se necesitan

Definir los componentes del blockchain a través de una clase partiendo desde el bloque inicial “génesis”, lista de bloques, nuevos bloques. Con esto se definen los bloques dentro de la cadena Figura 5.3

```
class Blockchain:
#definir todos los componentes del bch
    def __init__(self):    #LISTA DE BLOQUES
        self.chain = []    #iniciar el bloque
        self.create_block(proof = 1, previous_hash = '0')       #BLOQUE GENESIS

    def create_block(self, proof, previous_hash):#define el nuevo bloque que hemos creado
        block = {'index': len(self.chain) + 1,
                 'timestamp': str(datetime.datetime.now()),
                 'proof': proof,
                 'previous_hash': previous_hash}
        self.chain.append(block)
        return block
                            #con esto tenemos el bloque ahora adjuntar en la cadena
```

Figura 5.3 Clase blockchain

Blockchain como una clase, donde se definen todos los componentes de una blockchain válida

- ✓ Bloque génesis
- ✓ Cadena en función init
- ✓ Función para crear los bloques
- ✓ Agregar algoritmos que permita saber que el blockchain es sólido, seguro y resistente a hackers
- ✓ Luego con self especificamos que las variables que introducimos hacen referencia al objeto
- ✓ Self.chain contiene los bloques
- ✓ Definir el nuevo bloque, para ello un diccionario

4 claves esenciales para el éxito de una blockchain programadas en Figura 5.4

- ✓ Índice del bloque
- ✓ Timestamp
- ✓ Proof
- ✓ Hash previo

El retorno del bloque anterior es fundamental para la relación de la cadena, se Implementa la función de bloque anterior (-1) para obtener el último bloque minado dentro de la cadena Figura 4

```
24      def get_previous_block(self):       #funcion obtneer el bloque anterior
25          return self.chain[-1]             #·para obtener el bloque anterior
```

Figura 5.4 Obtener el bloque anterior

La prueba de trabajo (proof of work) requiere que todos sus mineros intenten resolver un problema complejo, y el ganador se determina por los dispositivos de hardware más potentes. La función chequea una a una las posibles pruebas previas hasta encontrar el correcto y retornar la nueva prueba de trabajo. Figura 5.5

```
27      def proof_of_work(self, previous_proof):
28          new_proof = 1
29          check_proof = False
30          while check_proof is False:
31              hash_operation = hashlib.sha256(str(new_proof**2 - previous_proof**2).encode()).hexdigest()
32              if hash_operation[:4] == '0000':
33                  check_proof = True
34              else:
35                  new_proof += 1
36          return new_proof
```

Figura 5.5 Función proof of work

- ✓ Los mineros resuelven un problema difícil de resolver y fácil de verificar
- ✓ Para crear un nuevo proof tener en consideración el proof anterior
- ✓ Un ciclo de falsedad, itera hasta encontrar el proof que resuelva el problema
- ✓ Creando el proof con 4 ceros por delante va a aumentar la dificultad del problema que tiene que resolver dicho minero
- ✓ Retorna un SHA256

La función hash permite tener la correcta prueba de trabajo verificando el hash previo de el bloque en particular y los bloques de toda la cadena Figura 5.6

```
38      def hash(self, block):
39          encoded_block = json.dumps(block, sort_keys = True).encode()
40          return hashlib.sha256(encoded_block).hexdigest()
```

Figura 5.6 Chequeo

- ✓ Que todos tengan la correcta prueba de trabajo osea correcto proof_of_word
- ✓ Previous hash es igual a previous hash de todos los bloques

La función is chain valid informa la validez de la cadena de manera eficiente en un modelo de tipo blockchain, permite declarar la validación por medio de un condicional (if) además de un ciclo while que determina a su vez validez de la cadena de acuerdo a la prueba previa. Figura 5.7

```
    def is_chain_valid(self, chain):
        previous_block = chain[0]
        block_index = 1
        while block_index < len(chain):
            block = chain[block_index]
            if block['previous_hash'] != self.hash(previous_block):
                return False
            previous_proof = previous_block['proof']
            proof = block['proof']
            hash_operation = hashlib.sha256(str(proof**2 - previous_proof**2).encode()).hexdigest()
            if hash_operation[:4] != '0000':
                return False
            previous_block = block
            block_index += 1
        return True
```

Figura 5.7 Declaración if para verificar la información del blockchain

- ✓ Si el Hashs previo es igual entonces con esto finalizamos el primer paso para crear una blockchain

- ✓ Ahora la funcionalidad de poder ser minado:

4 cosas para poder interactuar

Una web app permite ser visible en postdam con la línea de código y así interactuar. figura5.8

```
app = Flask(__name__)
```

Figura 5.8 Flask web

- ✓ Primero una flask web app para interactuar con la blockchain.

Es necesario crear un valor de petición llamado blockchain para que sea posible llamar la cadena de forma visual se observa en la Figura 5.9

```
blockchain = Blockchain()
```

Figura 5.9 Llamar cadena

- ✓ Hacer un blockchain para llamar la cadena

Con el método GET se llama la función de minar un bloque de esta manera la función mine_block permite hacer una solicitud a la estructura de minado estableciendo cada una de las esencias de blockchain, así como un archivo de tipo json para ser visible en postdam el código de la función minar un bloque Figura 5.10

```
#minando un bloque nuevo
@app.route('/mine_block', methods=['GET'])

def mine_block():
    previous_block = blockchain.get_previous_block()
    previous_proof = previous_block['proof']
    proof = blockchain.proof_of_work(previous_proof)
    previous_hash = blockchain.hash(previous_block)
    block = blockchain.create_block(proof,previous_hash)
    response = {'message':'Felicidades, haz minado un bloque!',
                'index':block['index'],
                'timestamp':block['timestamp'],
                'proof':block['proof'],
                'previous_hash':block['previous_hash']}
    return jsonify(response), 200
```

Figura 5.10 Primer Get request para minar el primer bloque

- ✓ Formato json para ser mostrado en postman

En la función get chain el método get realiza una petición esta vez para obtener una vista previa de la cadena completa, determina la longitud de dicha cadena como se observa en la figura 5.11

```
#  Cadena Completa
@app.route('/get_chain', methods=['GET'])
def get_chain():
    response = {'chain':blockchain.chain,
                'length':len(blockchain.chain)}
    return jsonify(response), 200
```

Figura 5.11 Get requets para trabajar toda la cadena

- ✓ Get chain ver cadena completa

- ✓ Completa la opción de minar el primer bloque

Para correr la web site local se añade la línea de código, con la dirección del puerto donde estará corriendo el código, el usuario hará las peticiones Figura 5.12

```
# Corriendo el App

app.run(host='0.0.0.0', port='5000')
```

LSP Python: ready conda: base (Pyth

Figura 5.12 El host disponible es perfecto para blockchain y el puerto del nodo

Chequeo de validez de blockchain. Esta función hace una revisión minuciosa del algoritmo, evalúa los algoritmos y determina una validez concreta por parte del código. Para completar la blockchain Figura 5.13

```
95              # Chequeando validez de cadena de bloques
96      @app.route('/is_valid', methods=['GET'])
97      def is_valid():
98          is_valid = blockchain.is_chain_valid(blockchain.chain)
99          if is_valid:
100             response = {'message':'Todo bien. El BLockchain es valido'}
101         else:
102             response = {'message':' tenemos un problema. El blockchain no es valido!'}
103         return jsonify(response), 200
```

Figura 5.13 Función verificamos la validez de la cadena

5.2.2 Se convierte la blockchain en una criptomoneda

El código de blockchain en un nuevo documento Figura 5.14, guardar con el nombre que recibe la criptomoneda. Figura 5.15 "clinic_historycoin" por el uso en la implementación de las historias clínicas.

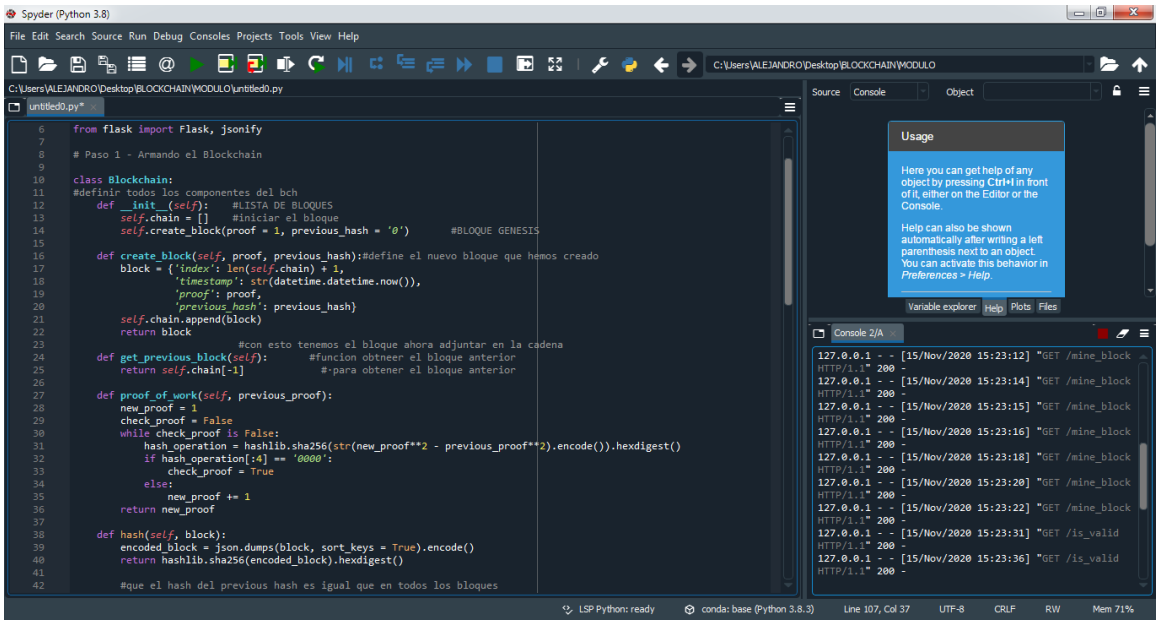


Figura 5.14 El código en un nuevo file

Figura 5.15 Guardar con el nombre que valla recibir la criptomoneda en este caso

La funcionalidad de criptomonedas requiere nuevos paquetes, es importante y se agregan con los demás paquetes. Figura 5.16

```
import json
from flask import Flask, jsonify, request
import requests
from uuid import uuid4
from urllib.parse import urlparse
```

Figura 5.16 Importar un par de paquetes requeridos para la adaptación de la criptomoneda

5.2.2.1 Una criptomoneda en 3 partes

- Se armar blockchain
- Minar blockchain
- Descentralizar el blockchain

Una criptomoneda la hace la transacción del blockchain asegurada por la encriptación, se agregan en la clase blockchain las transacciones Figura 5.17

```
class Blockchain:

    def __init__(self):
        self.chain = []
        self.transactions = []
        self.create_block(proof = 1, previous_hash = '0')
        self.nodes = set()
```

Figura 5.17 Agregar las transacciones

En la función crear bloque se agregan las transacciones Figura 5.18
Se agrega la función transactions, donde se establece los términos de dichas transacciones (sender, receiver, amount) Figura 5.18

```
    def create_block(self, proof, previous_hash):
        block = {'index': len(self.chain) + 1,
                 'timestamp': str(datetime.datetime.now()),
                 'proof': proof,
                 'previous_hash': previous_hash,'transactions':self.transactions}
        self.transactions = []
        self.chain.append(block)
        return block
    #lista trabsacciones
    def add_transactions(self, sender, receiver, amount):
        self.transactions.append({'sender':sender,'receiver':receiver,'amount':amount})
        previous_block = self.get_previous_block()
        return previous_block['index']+1
```

Figura 5.18 Formato para las transacciones (enviador, recipiente, cantidad enviada)

5.2.2.2 Append para agregar las tres llaves a las transacciones (sender, receiver, amount)

La blockchain está contenida por nodos que ejecutan el mismo algoritmo, agregar nodos a la red mediante un ciclo, ejecutando un pequeño modelo de petición y respuesta por parte del algoritmo, así como un condicional para la validez de cada nodo dentro de la red, una

vez pertenezca a la red podrá ejecutar el protocolo de consenso y posteriormente chequear toda la red. Figura 5.19

```
        for node in network:
            response = requests.get(f'http://{node}/get_chain')
            if response.status_code == 200:
                length = response.json(['length'])
                chain = response.json(['chain'])

                if length > max_length and self.is_chain_valid(chain):
                    max_length = length
                    longest_chain = chain

            if longest_chain:
                self.chain = longest_chain
                return True
```

Figura 5.19 Node serán varios nodos

Necesariamente se dirige la petición a una dirección única aleatoria, con el llamado respectivo a blockchain. Figura 5.20

```
#creando una dir para el nodo en el puerto 5000

node_address = str(uuid4()).replace('-','')
blockchain = Blockchain()
```

Figura 5.21 Una dirección única aleatoria

En la función de minar bloque debe adicionarse los parámetros regulares de la transacción como: cantidad, quien envía, quien recibe. La importancia de una transacción lógica y coherente dentro de un bloque minado. Figura 5.22

```
def mine_block():
    previous_block = blockchain.get_previous_block()
    previous_proof = previous_block['proof']
    proof = blockchain.proof_of_work(previous_proof)
    previous_hash = blockchain.hash(previous_block)
    blockchain.add_transactions(sender= node_address, receiver= 'Alejandro', amount=1)
    block = blockchain.create_block(proof,previous_hash)
    response = {'message':'Felicidades, haz minado un bloque!',
                'index':block['index'],
                'timestamp':block['timestamp'],
                'proof':block['proof'],
                'previous_hash':block['previous_hash'],'transactions':block['transactions']}
    return jsonify(response), 200
```

Figura 5.22 Agregar cantidad y quien recibe la transacción

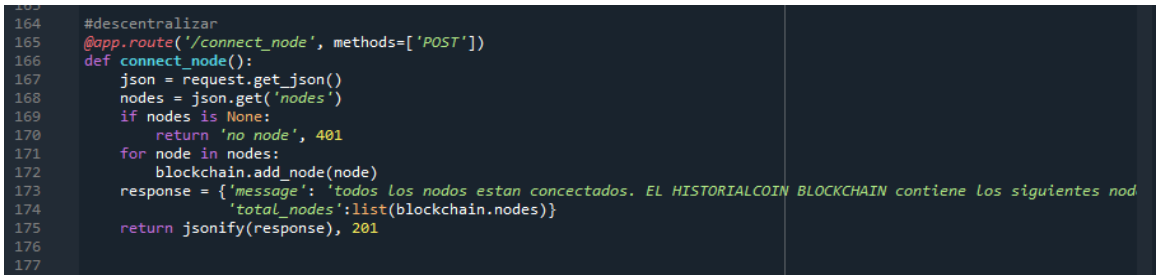
Agregar por medio de un método POST una función app route de transactions, la cual será llamada una vez se conceda la petición de realizar una transacción Figura 5.23

```
@app.route('/transaction', methods=['POST'])
def add_transactions():
    json = request.get_json()
    transaction_keys = ['sender', 'receiver', 'amount']
    if not all(key in json for key in transaction_keys):
      return 'Algun elemento de la transaccio esta faltando', 400

    index = blockchain.add_transactions(json['sender'],json['receiver'],json['amount'])
    response = {'message':f'la transaccion sera añadida al bloque {index}'}
    return jsonify(response), 201
```

Figura 5.23 agregando nuevas transacciones con el método POST

5.3 Descentralizar el blockchain

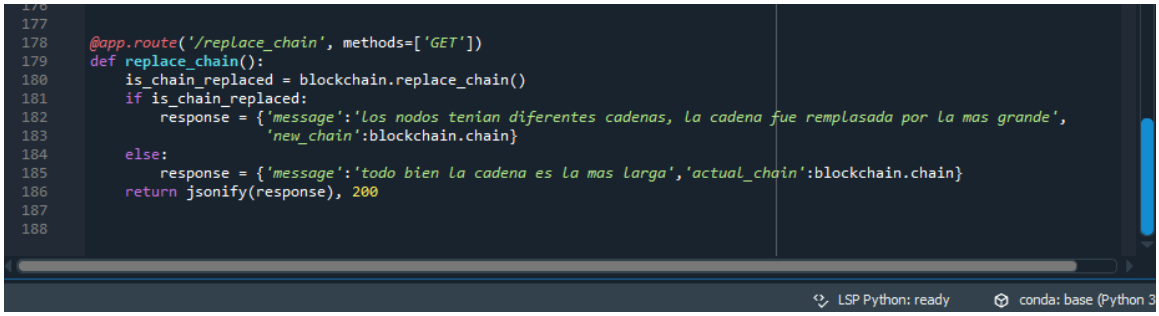
La función connect node, permite establecer una estructura dedicada a la coneccion con nuevos nodos dentro de la red distribuida, los nodos conectados podrán ser anfitriones de los protocolos de blockchain, dando un ambiente de descentralización a nivel tipológico y de acuerdo a sus características una red distribuida Figura 5.24



```
#descentralizar
@app.route('/connect_node', methods=['POST'])
def connect_node():
    json = request.get_json()
    nodes = json.get('nodes')
    if nodes is None:
        return 'no node', 401
    for node in nodes:
        blockchain.add_node(node)
    response = {'message': 'todos los nodos estan concectados. EL HISTORIALCOIN BLOCKCHAIN contiene los siguientes nod
                'total_nodes':list(blockchain.nodes)}
    return jsonify(response), 201
```

Figura 5.24 Conectar los nodos de la lista

Agregar consenso de reemplazar cadenas más cortas, el algoritmo de consenso evalúa de manera lógica las peticiones de la red, una de estas características esenciales en la red blockchain permite diagnosticar la red con una reseña de longitud: Determina la cadena más larga en los nodos de la red y reemplaza las cadenas cortas por la ya determinada y validad cadena más larga. Figura 5.25



```
@app.route('/replace_chain', methods=['GET'])
def replace_chain():
    is_chain_replaced = blockchain.replace_chain()
    if is_chain_replaced:
        response = {'message':'los nodos tenian diferentes cadenas, la cadena fue remplasada por la mas grande',
                    'new_chain':blockchain.chain}
    else:
        response = {'message':'todo bien la cadena es la mas larga','actual_chain':blockchain.chain}
    return jsonify(response), 200
```

LSP Python: ready conda: base (Python 3

Figura 5.25 En caso de necesitar reemplazar la cadena o no

Con todos los algoritmos de blockchain verificados y validados, se adicionan unas secciones de códigos que le permiten verse como una aplicación más precisa y le da una practicidad a nivel visual, con el objetivo que los agentes del prototipo puedan interactuar con la blockchain orientada a las transacciones de historiales clínicos por redes de tipología distribuidas, en otras palabras es la parte del algoritmo donde el desarrollo tiene enfoque en los usuarios tales como pacientes y médicos dentro del sistema de salud del Hospital San Juan De Dios de Pamplona. Figura el servidor registra las solicitudes de acceso a la blockchain.

```
93
94  ################servidor y registro###################################
95  app = Flask(__name__)
96  app.config['SECRET_KEY'] = 'thisisasecret'
97  app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///db.sqlite3'
98  app.config['SECURITY_PASSWORD_SALT'] = 'thisisasecretsalt'
99  node_address = str(uuid4()).replace('-','')
100 blockchain = Blockchain()
101 db = SQLAlchemy(app)
102
103 roles_users = db.Table('roles_users',
104     db.Column('user_id', db.Integer, db.ForeignKey('user.id')),
105     db.Column('role_id', db.Integer, db.ForeignKey('role.id')))
106
```

Figura 5.26 Esta función se denomina fábrica de aplicaciones.

Cualquier configuración, registro y otra configuración requerida por los agentes de la cadena en la aplicación se realizará dentro de la función y luego volverá a la aplicación. Figura 5.27

```
108 class User(db.Model, UserMixin):
109     id = db.Column(db.Integer, primary_key=True)
110     email = db.Column(db.String(100), unique=True)
111     password = db.Column(db.String(255))
112     active = db.Column(db.Boolean)
113     confirmed_at = db.Column(db.DateTime)
114     roles = db.relationship(
115         'Role',
116         secondary=roles_users,
117         backref=db.backref('users', lazy='dynamic')
118     )
119
120 class Role(db.Model, RoleMixin):
121     id = db.Column(db.Integer, primary_key=True)
122     name = db.Column(db.String(40))
123     description = db.Column(db.String(255))
124
125 user_datastore = SQLAlchemyUserDatastore(db, User, Role)
126 security = Security(app, user_datastore)
127
```

Figura 5.27 Flask-User distingue los grupos de información de usuario

- ✓ Permite a los desarrolladores almacenar datos de autenticación, correo electrónico e información del usuario en uno o más modelos de datos

- ✓ Requiere que la información del rol del usuario se almacene en el modelo de datos del rol y en la tabla de asociación del rol del usuario.

La tabla de roles contiene el nombre de cada rol. El nombre se comparará con el modificador de función @roles_required de manera sensible a mayúsculas y minúsculas. Figura 5.28

```python
@app.route('/register', methods=['POST', 'GET'])
def register():
    if request.method == 'POST':
        user_datastore.create_user(
            email = request.form.get('email'),
            password = hash_password(request.form.get('password'))
        )
        db.session.commit()
        return redirect(url_for('profile'))
    return render_template('register.html')
```

Figura 5.28 Contenido en una URL específica.

La ruta del registro se refiere al patrón de URL de la aplicación, donde se registrarán los usuarios que participarán en la cadena, con un email, password. Figura 5.29

```python
@app.route('/profile')
@login_required
def profile():
    return render_template('profile.html')

@app.route('/logout')
def logout():
    logout_user()
    return redirect(url_for('profile'))
```

Figura 5.29 Rutas que resuelven el profile y el logout

Con los algoritmos del sistema blockchain se hizo una rápida migración del ambiente virtual de spyder a PyCharm debido a la rápida integración de este entorno con librerías y funciones fundamentales para desplegar blockchain (cliente y servidor). (Moujahid, 2018)

La programacion por parte del cliente o usuario estaría compuesta por funciones y librerías que generan las interacciones dinámicas como peticiones, allí es donde se realizan las solicitudes de transacciones de los médicos o pacientes, de igual manera un sistema de autenticador de identidad realiza una comunicación con el servidor de manera que genera las llaves públicas y privadas con las que estará en la red blockchain como usuario.

```
USER_FILE_NAME = 'users.data'


class User(object):
    def __init__(self, email, key=None):
        self.email = email
        self.key = key
        if key is None:
            self.key = pyotp.random_base32()

    def save(self):
        if len(self.email) < 1:
            return False

        users = pickle.load(open(USER_FILE_NAME, 'rb'))
        if self.email in users:
            return False
        else:
            users[self.email] = self.key
            pickle.dump(users, open(USER_FILE_NAME, 'wb'))
            return True
```

Figura 5.30 Código blockchain cliente (Moujahid, 2018)

Se define la función de autenticador de identidad con el fin de generar un acceso correcto y validado a un área de operación blockchain como se observa en la Figura 5.31

```
    def authenticate(self, otp):
        p = 0
        try:
            p = int(otp)
        except:
            return False
        t = pyotp.TOTP(self.key)
        return t.verify(p)

    @classmethod
    def get_user(cls, email):
        users = pickle.load(open(USER_FILE_NAME, 'rb'))
        if email in users:
            return User(email, users[email])
        else:
            return None
```

Figura 5.31 Función authenticate

Esta función determina una validación por medio del correo que será el que interprete la autenticación en la aplicación de google authenticator Figura 5.32

```
def code(email):
    """
    Returns the one-time password associated with the given user for the
    current time window. Returns empty string if user is not found.
    """
    u = User.get_user(email)
    if u is None:
        return ''
    t = pyotp.TOTP(u.key)
    return str(t.now())

class Transaction:

    def __init__(self, sender_address, sender_private_key, recipient_address, value):
        self.sender_address = sender_address
        self.sender_private_key = sender_private_key
        self.recipient_address = recipient_address
        self.value = value

    def __getattr__(self, attr):
        return self.data[attr]

    def to_dict(self):
        return OrderedDict({'sender_address': self.sender_address,
```

Figura 5.32 Función code (email)

Esta función genera la llave privada para abrir la transacción Figura 5.33

```
    def sign_transaction(self):
        """
        Sign transaction with private key
        """
        private_key = RSA.importKey(binascii.unhexlify(self.sender_private_key))
        signer = PKCS1_v1_5.new(private_key)
        h = SHA.new(str(self.to_dict()).encode('utf8'))
        return binascii.hexlify(signer.sign(h)).decode('ascii')


app = Flask(__name__)


@app.route('/')
def index():
    return render_template('./index.html')


@app.route('/make/transaction')
def make_transaction():
    return render_template('./make_transaction.html')
```

Figura 5.33 Función sign transaction

Permite ver las transacciones realizadas por el usuario validado por el autenticador de identidad de este lado del modelo blockchain, permite ver las transacciones agregadas a la historia clínica del paciente Figura 5.34

```python
@app.route('/view/transactions')
def view_transaction():
    return render_template('./view_transactions.html')


@app.route('/wallet/new', methods=['POST'])
def new_wallet():
    u = User.get_user(request.form['correo'])
    if u is None:
        return 'Correo no registrado', 400
    else:
        otp = request.form['token']
        if u.authenticate(otp):
            random_gen = Crypto.Random.new().read
            private_key = RSA.generate(1024, random_gen)
            print('hola')
            public_key = private_key.publickey()
            response = {
                'private_key': binascii.hexlify(private_key.exportKey(format='DER')).decode('ascii'),
                'public_key': binascii.hexlify(public_key.exportKey(format='DER')).decode('ascii')
            }
        else:
            return 'Token invalido', 400
```

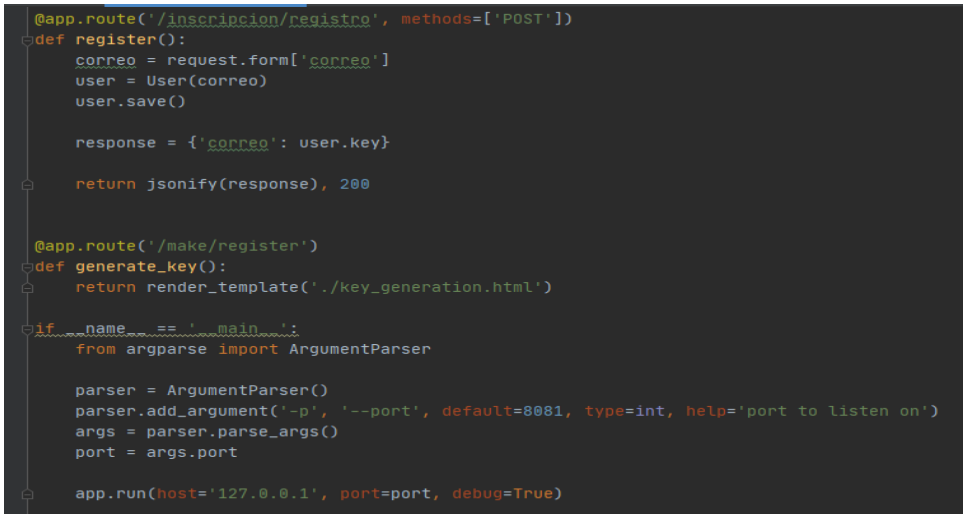
Figura 5.34 Función view transations

Esta función permite generar transacciones por medio del método post, estableciendo un modelo de peticiones las cuales resolverá el algoritmo por medio de la programación de parte del servidor Figura 5.35

```python
@app.route('/generate/transaction', methods=['POST'])
def generate_transaction():
    sender_address = request.form['sender_address']
    sender_private_key = request.form['sender_private_key']
    recipient_address = request.form['recipient_address']
    value = request.form['amount']

    transaction = Transaction(sender_address, sender_private_key, recipient_address, value)

    response = {'transaction': transaction.to_dict(), 'signature': transaction.sign_transaction()}

    return jsonify(response), 200


@app.route('/inscripcion/registro', methods=['POST'])
def register():
    correo = request.form['correo']
    user = User(correo)
    user.save()

    response = {'correo': user.key}

    return jsonify(response), 200
```

Figura 5.35 Función generate transation

Esta determina los registros que se desempeñan como usuarios de la cadena inscripción y registro de nuevos pacientes o medios en el ecosistema blockchain en el prototipo de historiales clínicos Figura 5.36



```python
@app.route('/inscripcion/registro', methods=['POST'])
def register():
    correo = request.form['correo']
    user = User(correo)
    user.save()

    response = {'correo': user.key}

    return jsonify(response), 200


@app.route('/make/register')
def generate_key():
    return render_template('./key_generation.html')

if __name__ == '__main__':
    from argparse import ArgumentParser

    parser = ArgumentParser()
    parser.add_argument('-p', '--port', default=8081, type=int, help='port to listen on')
    args = parser.parse_args()
    port = args.port

    app.run(host='127.0.0.1', port=port, debug=True)
```

Figura 5.36 Función inscripción registro.

Resultados

Los resultados del proyecto se pueden presentar mediante imágenes, videos, video llamadas, conferencias, publicaciones, etc. El capítulo ofrece resultados visuales a través de una secuencia de imágenes, se puede dividir en contextualización del prototipo, estructura de código, adición de innovación y contribuciones tecnológicas y la presentación y defensa de los resultados. Los resultados presentados a través de interfaz gráfica tienen una estructura similar, pero pueden mostrar claramente el desarrollo profesional y determinista del código para introducir varias ilustraciones sin límites de tiempo estrictos para los resultados valorados.

En cualquier caso, independientemente de cómo se presentan los resultados del prototipo, es importante indicar que este prototipo se diseña con el objetivo de implementar la tecnología blockchain en las historias clínicas de los usuarios del Hospital San Juan De Dios, es un objetivo que cumple con características específicas de seguridad y validación de la información, estos resultados son precisos y absolutos pues tiene como resultado la representación tecnológica y validación de los algoritmos que se citan, esto proporcionará una estructura adecuada para la presentación de los resultados.

En la actualidad, es importante que un proyecto de investigación no solo defina el tipo de resultados que aspira a alcanzar en el orden de conocimiento, sino también en términos de posibles efectos o impactos a sociales, administrativos y profesionales. Por lo tanto, no solo debe especificar los objetivos de la implementación de blockchain en los historiales de salud, sino también ser ampliamente conocida por los miembros que actuarán en la cadena, dichos participantes estarán en interacción con el prototipo, tanto los usuarios (cliente, médico) están en control de acceder mediante una interfaz gráfica del ordenador a hacer peticiones y respuesta al servidor local, quien está corriendo el código y también debe presentar una serie de resultados desde la perspectiva de demostrar su utilidad a determinadas comunidades de usuarios o determinadas operación multi usuarios y administradores de la cadena.

Prueba blokchain en Python figura

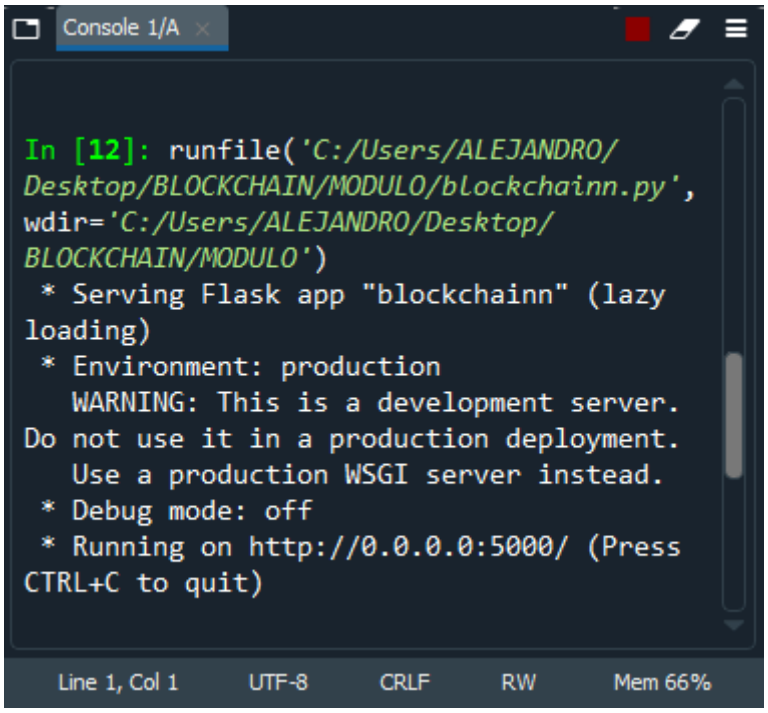


Figura 6.0 Corriendo el servidor flask con Python

Una vez corriendo el algoritmo en postman se puede visualizar el despliegue del código figura

- ✓ http://127.0.0.1:5000/get_chain url para ver la cadena

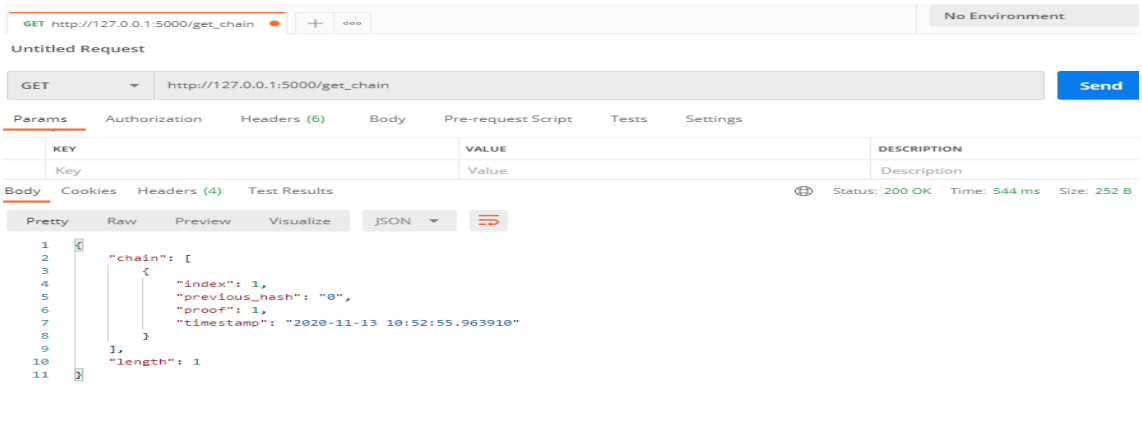


Figura 6.1 Postman bloque genesis

Se mina el primer bloque con l url siguente posteriorente se visualiza en postman Figura 6.2

- ✓ url minar un bloque http://127.0.0.1:5000/mine_block

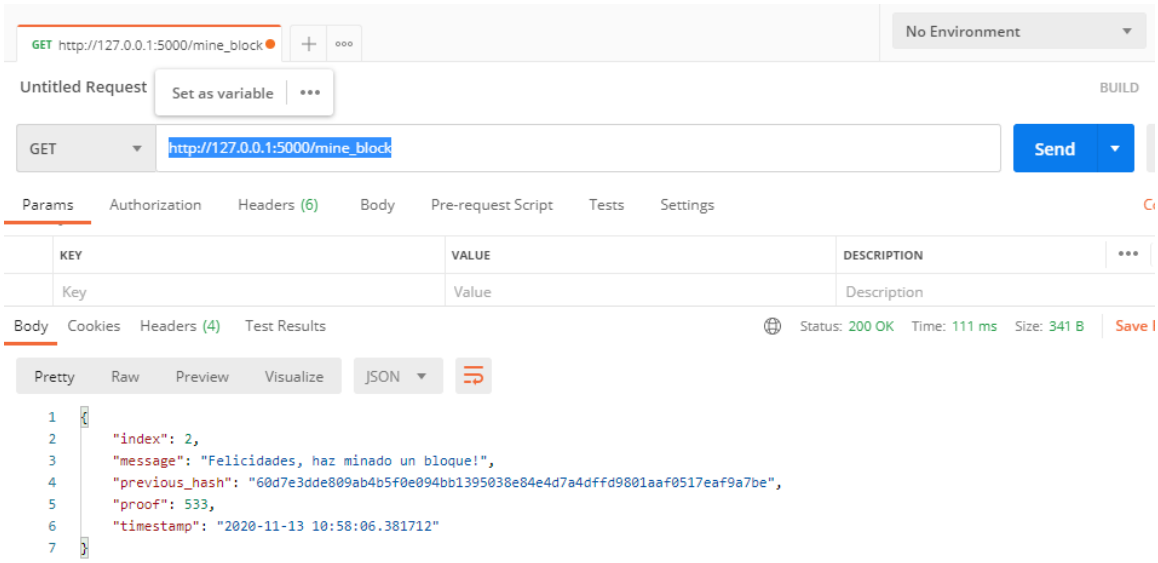


Figura 6.2 Primer bloque minado

Después de minar varios bloques para ver toda la cadena se utiliza la url siguiente y en postman Figura 6.3

- ✓ url http://127.0.0.1:5000/get_chain

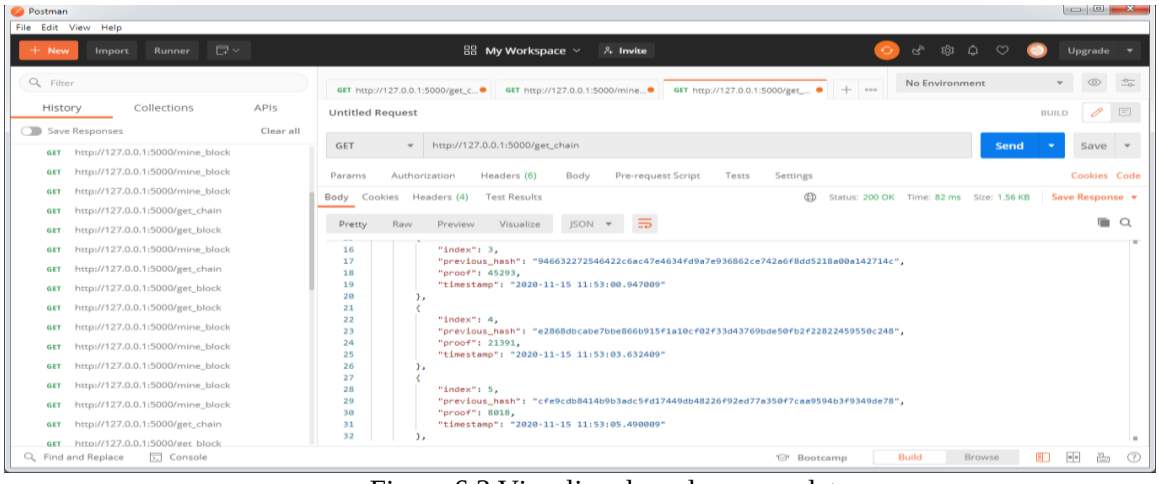


Figura 6.3 Visualizar la cadena completa

Para validar la cadena se utiliza la siguiente url, se visualiza en postman

✓ En postman para validar la cadena
url: http://127.0.0.1:5000/is_valid

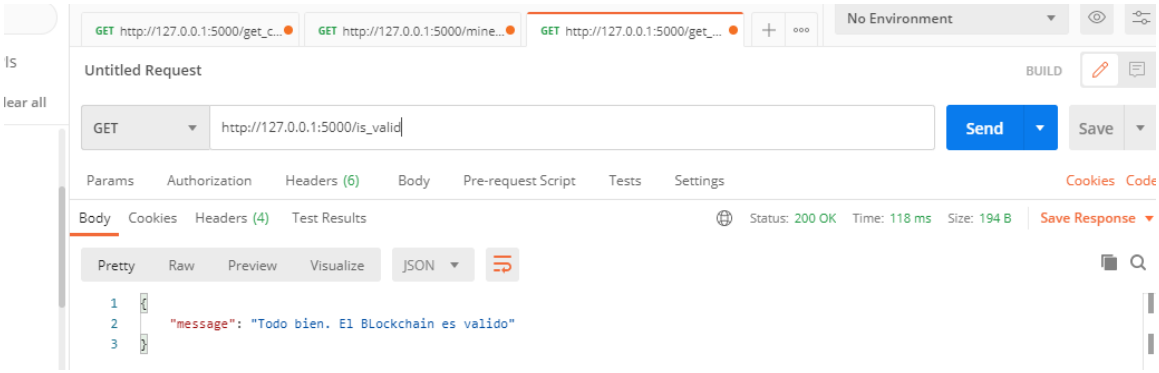


Figura 6.5 Validación de cadena

✓ Esta funcionando todo bien

Abrir el navegador

url http://127.0.0.1:5000/ blockchain server

La interfaz grafica vista en la figura, permite visualizar el área de operación por parte del administrador de la red, donde se uica el nombre del prototipo (Blockchain Historias Clinicas Hospital San Juan De Dios), Areas de ubicación de bloques por minar y en la parte inferiro las transacciones ya validadas y minadas en blockchacin. Esto para el apartado de minar bloque.

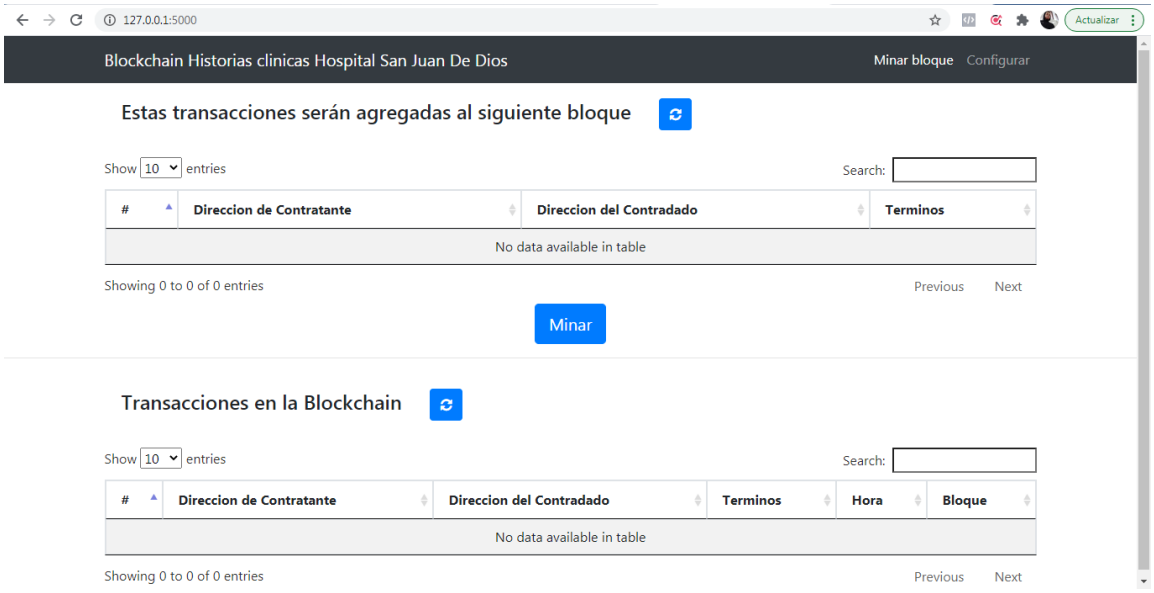


Figura 6.6 Interfaz gráfica blockchain server

En el apartado de configurar figura, permite una vista previa de agregar nodos para dar el enfoque a una red de tipo distribuida, margen importante para resaltar en blockchain, cada nodo de estos puede estar corriendo en cualquier servidor a nivel mundial para el desarrollo de este prototipo corre de manera local.

Figura 6.6 Interfaz configurar

Manual de usuario

Por parte del cliente la siguiente url

url http://127.0.0.1:8081/ blockchain cliente

La visaulizacion grafica evidencia el area de interaccion por parte del cliente el cual puede ser paciente o medico(Zona historias clinicas Hospital San Juan De Dios (Blockchain)) Figura 6.7

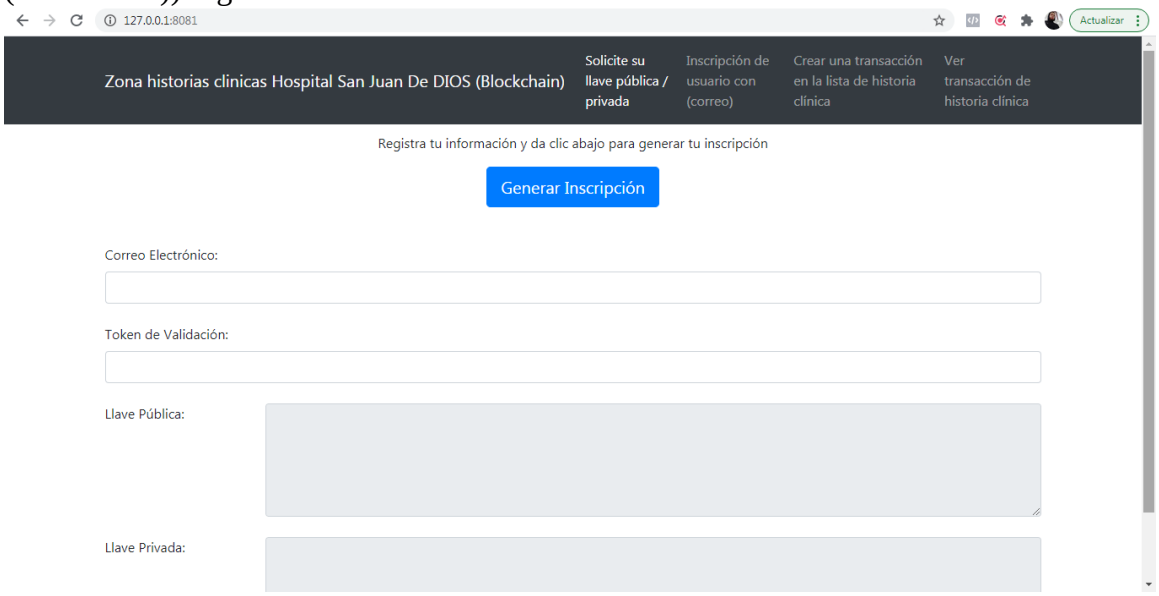


Figura 6.7 Interfaz gráfica blockchain cliente

En el apatado de inscripcion de nuevo usuario (paciente / medico (correo)),es donde los usuarios roles del prototipo hacen el registro por medio del auntenticador de identidad de google

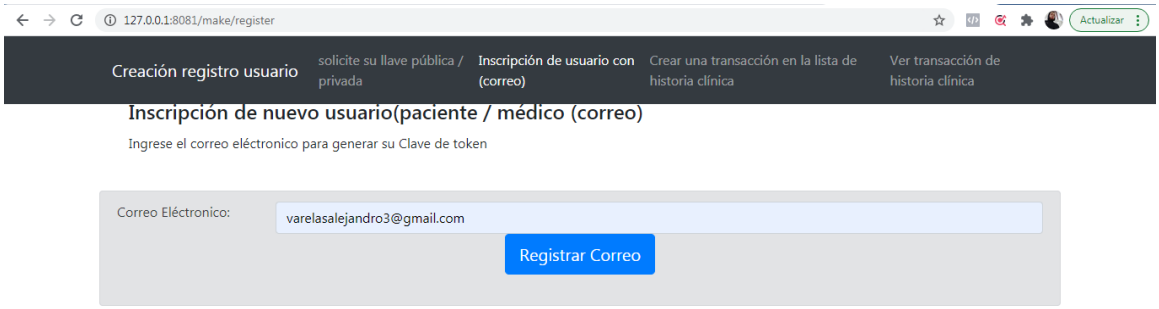


Figura 6.8 Agregar nuevos nodos a la cadena

En la sección de registro de correo electrónico, se debe agregar el correo que usaría uno de los usuarios que participará del blockchain, posteriormente registrar. En un dispositivo de acceso a internet, buscar google autenticador, registrar correo y agregar la llave de acceso con esto se tiene un usario identificado listo para operar la red y desplegar transacciones de tipo clínicas Figura 6.9

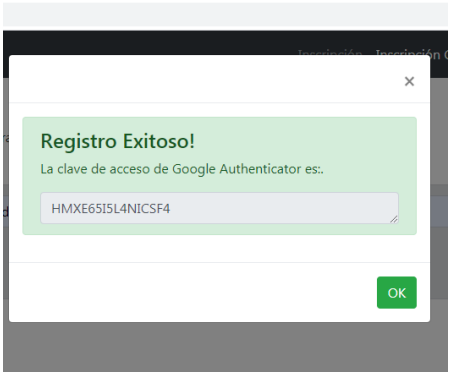


Figura 6.9 Registro exitoso

Esto despliega un mensaje que indica que el registro será exitoso una vez se agregue la clave de acceso de google authenticator (google authenticator no permite capturar pantalla), una vez allí basta con agregar el nombre de usuario y la clave de acceso, con esto empezará a asignar un token dinámico, que cambiará cada 30 segundos, un número de 6 dígitos para la accesibilidad a la Interacción con blockchain.

En la figura se genera las llaves privadas y publicas de cada usuario con el correo registrado y el autenticador de google, una vez visualiza las llaves considere guardar de manera segura pues será las llaves de operación para desplegar las transacciones de manera exitosa

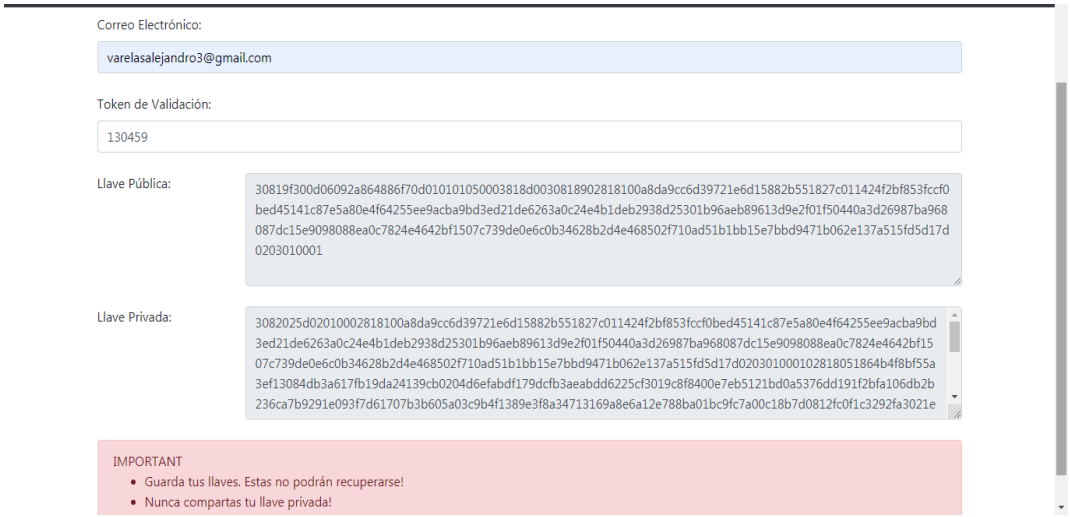


Figura 6.10 Llaves

- ✓ Para generar una inscripción con el email y el token de validación se generarán las llaves (Pública y Privada) de este actor de la cadena.
- ✓

Crear transacción

Una vez registrado en el blockchain de historias clínicas del hospital, se procede a realizar las primeras transacciones, importante contemplar

En la figura, el formulario pretende la información general del paciente, direcciones de llave publica y privada del medico y paciente, nombre, documento entre otros

En la figura, el formulario pide otros datos generales como nombre del medico, identificación del mismo, y además una casilla importante es agregar documento a la transacicion de historia clínica en esta se podrá adjntar documentos de suma importancia en el sistema de salud como radiografías, examnes, registros de electrocardigramas y demás información que por consiguiente se puede representar por un documento o carpeta de margen necesaria y obligatoriadentro de el sistema de salud del Hospital San Juan De Dios de Pamplona

La información de la Figura 6.11 y Figura 6.12, son los datos de las trasacciones los cuales van cifrados por medio de criptografía digital lo que representa el cumplimiento de los objetivos del prototipo a nivel general.

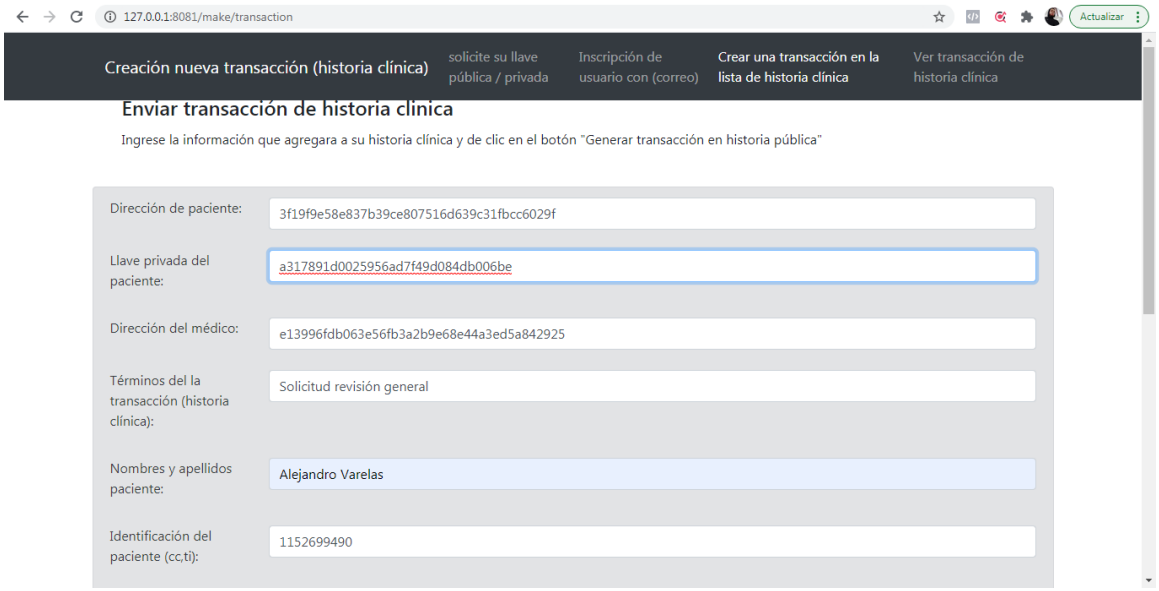


Figura 6.11 Formulario transacciones

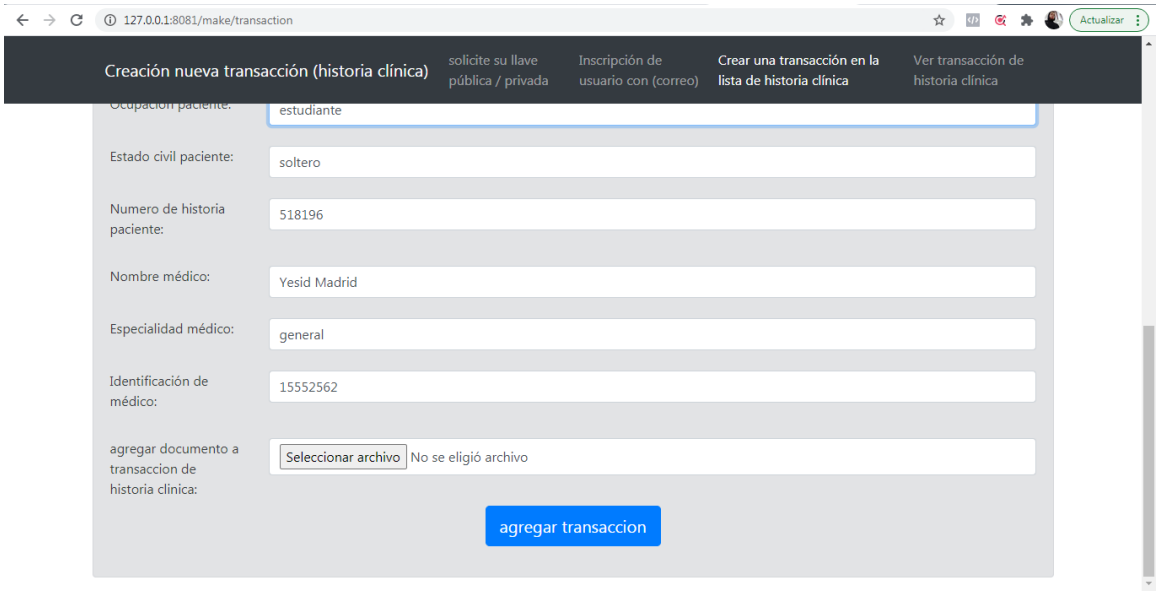


Figura 6.12 Formu.lario de transacción

Para establecer el primer bloque se describe la información que va desplegar esta transacción con la dirección del contratante, llave privada del contratante, dirección del contratado y términos del contrato o transacción de esta manera estará listo el formulario de solicitud de la nueva transacción. Con esto la transacción se añadirá a la lista de bloques por mina

Minando bloques

Como se observa en la figura la lista se visualiza dirección del paciente, dirección del medico y términos con esto solo resta minar este bloque para que abandone la lista de bloques por minar y conforme una transacción ya validada y minada, esta se verá en la lista de transacciones blockchain.

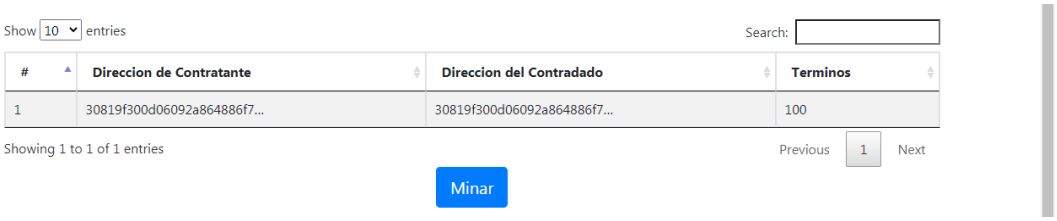


Figura 6.13 Lista de bloques por minar

En la figura se observa como la transaccion clinica ya esta establecida en el blockchain, como un bloque establecido enviador por un miembro de la cadena y pertenece a las transacciones del paciente, es de esta manera que se gestiona las transacciones de blockchain en la red.

Figura 6.14 Lista de bloques minados

De esta manera se llega al punto de salida de la implementación de blockchain orientado a las historias clínicas, es así como el prototipo de esta tecnología resulta ser un éxito para la interaccion en un ecosistema medico para el Hospital San Juan De Dios De Pamplona, siguiendo y verificando las características que permite orientar la tecnología a las transacciones para historiales clínicos.

Prototipo de transacciones a través de tecnología de cadena de bloques relacionando partícipes específicos para el ambiente hospitalario con el fin de dar soporte en el sistema innovador de datos basado en tecnología blockchain, a través de un enfoque colaborativo e inteligente de la atención médica permitiendo a cada usuario una autonomía e inmutabilidad sobre el valor que tiene sus historiales clínicos, con el fin de avanzar dentro del desarrollo de la salud pública y las alternativas fuera del mecanismo tradicional.

Conocer parte del historial de cada paciente permitirá detectar patrones que se manifiestan antes de ciertas enfermedades o averiguar cuáles son los tratamientos más efectivos. Gracias a ello, se podrá mejorar el sistema de prevención y cura llegando a salvar vidas humanas.

Las blockchains están diseñadas como sistemas distribuidos estándar que registran y protegen los archivos a través del uso de criptografía, resulta extremadamente difícil que alguien presente deseos de perturbe o cambie los datos si no dispone de la aprobación de todos los miembros de la red. Por lo tanto, la inmutabilidad es una de las características que permiten la creación de bases de datos incorruptibles para registros médicos.

Con lo que la arquitectura peer-to-peer empleada en los modelos que despliegan las blockchains, permite que todas las copias de los registros de un paciente sean sincronizadas entre sí cada vez que se llevan a cabo actualizaciones dentro de la misma, a pesar de encontrarse almacenadas en distintos ordenadores(nodos). De hecho, cada nodo de la red contiene una copia de toda la blockchain, y se comunica regularmente con el resto para asegurarse que los datos están actualizados y son auténticos. Por lo tanto, la descentralización y la distribución de datos son también aspectos importantes. Código de (Moujahid, 2018)

Conclusiones

Podemos implementar una red de registros médicos basada en blockchain y realizar funciones básicas. Mediante el uso de las funciones principales de la cadena de bloques (cifrado / hash y descentralización), los principales objetivos de esta investigación se lograron con éxito, proteger los registros médicos y proteger la privacidad del paciente. La tecnología Blockchain es una tecnología innovadora para implementar registros médicos y también puede contribuir a la investigación y el progreso de la atención médica en un futuro próximo.

Blockchain con la puesta en marcha de los algoritmos de este proyecto puede brindar funciones avanzadas del sistema de atención médica, esta idea e implementación se pueden expandir aún más en el futuro con la operatividad del algoritmo completo, como también agregando componentes adicionales en la Interacción con los actores de la cadena. Se pueden agregar varios departamentos como facturación, rastreo de medicamentos e incluso transporte, además puede ser de gran ayuda en la coyuntura actual de la pandemia 2020.

En el desarrollo del proyecto surgen múltiples situaciones las cuales estaban previstas desde la propuesta del mismo, se puede resaltar la escasez de recursos bibliográficos para la programación de algoritmos tan minuciosos como la encriptación de información, validación y verificación de blockchain, a pesar de que no es una tecnología nueva no cuenta con numerosos centros de datos significativos para desarrolladores o ingenieros que trabajan en ella, la mayoría de sus implementaciones se dirigen a otros ámbitos como dinero y contratos inteligentes, sin embargo con bases de programación sólida y la accesibilidad a un entorno de programación amplio y versátil, se puede desplegar una blockchain en un plazo considerable, y de igual manera se pueden resolver los problemas de compatibilidad que pueden surgir entre las diferentes versiones y actualizaciones de los sistemas y entornos de programación, además de que con la documentación de las diferentes versiones se puede compilar los algoritmos que en conjunto despegan una red blockchain.

Un criterio más realista permite concluir que una entidad gubernamental puede proyectar esta tecnología como solución a todos los problemas ya mencionados en el documento, con una inversión mediana, una revisión minuciosa y sobretodo que puede contrarrestar con un estado más sólido a medida que más profesionales decidan incursionar en la blockchain y además que cumplan con la experiencia que demanda mantener estable y escalable esta tecnología, con el objetivo de desarrollar su entorno de manera más sencilla y ejecutable, por parte de los usuarios que no tiene un conocimiento avanzado en los sistemas de software y telecomunicaciones.

En el área de las telecomunicaciones permite concluir que blockchain siendo una arquitectura de tipología de red distribuida, podrá aumentar la demanda en sistemas de telecomunicaciones y sistemas de software, como el desarrollo de los nodos mineros que serán protagonistas en las transacciones y en la dinámica de operaciones que exige el modelo de estas redes, siendo así de vital importancia para los ingenieros en el control total de los medios en que se realiza la comunicación y las altas demandas de ancho de banda que se requieren para que las redes distribuidas sean versátiles a la hora de estar en un funcionamiento del 100% de manera real, además de resolver cualquier altercado que pueda presentarse de manera lógica y física en la red.

Sin embargo, todavía existen muchos desafíos operativos y de investigación, tratando de integrar completamente la tecnología blockchain con los sistemas médicos existentes en este documento se planteó un prototipo que podría ser una solución viable para los agentes del estado más específicamente del hospital para implementar esta tecnología emergente que se desarrollara de manera más escalable en los próximos años, sin duda alguna el prototipo resalta su éxito en la ejecución y validación ya representada en la sección de resultados.

Lista de referencias

Bhushan, B., Sinha, P., Sagayam, K. M., & J, A. (2020). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers and Electrical Engineering*, *July 2019*, 106897. https://doi.org/10.1016/j.compeleceng.2020.106897

Blockchain, I. B. M., Cloud, I. B. M., Blockchain, I. B. M., & Cloud, I. B. M. (n.d.). *Healthchain lanza red basada en blockchain para unificar la historia clínica de los pacientes en América Latina*.

C. Chisaba. (2017). La gestión en salud a través del blockchain: una herramienta del futuro inmediato. *UnBosque*, *6*, 51–56. https://revistas.unbosque.edu.co/index.php/HEB/article/view/2619/2131

Chari, R. (2020). *No Covariance Structural Analysis of Health-Related Indicators in the Elderly at Home with a Focus on Subjective Health PerceptionTitle*. http://repositorio.unan.edu.ni/2986/1/5624.pdf

Chawla, C. (2020). Trust in blockchains: Algorithmic and organizational. *Journal of Business Venturing Insights*, *14*(July), e00203. https://doi.org/10.1016/j.jbvi.2020.e00203

Cies, R., Escolme, U., Mart, J. S., Inform, S., Escolme, U., Guti, A. O., Inform, S., Escolme, U., Hern, C., Ibarra, O., Investigador, D., & Escolme, U. (2020). *Acercamiento a la tecnología Blockchain y posibles aplicaciones en el sector salud en Colombia*. 11–24.

dinero. (2018). *blockchain sector salud publica*.

García-Morales, E. (2018). Luces y sombras sobre el impacto del blockchain en la gestión de documentos. *Anuario ThinkEPI*, *12*, 345. https://doi.org/10.3145/thinkepi.2018.58

Mellizo Gomez, D., & Minú Dussán, J. (2020). Modelo basado en Blockchain para la implementación de una historia clínica electrónica familiar. *Revista de Investigación En Tecnologías de La Información*, *8*(16), 10–22. https://doi.org/10.36825/riti.08.16.002

Omar Gutiérrez, Jeffreys J. Saavedra, P. M. W. y A. S. (2019). *BC-MED: Plataforma de registros médicos electrónicos sobre tecnología Blockchain*.

Piedra, U. L. (2018). Blockchain en el sector salud: Aplicaciones y ventajas. *Izertis*.

Pierro, D. (2017). *What Is the Blockchain? October*.

Quiroga Cruz, Jorge; Cubillos Herrera, S. (2018). Fundamentación de un modelo mediante la tecnología blockchain para el tratamiento de información en el área de vigilancia epidemiológica de la clínica Juan N . Corpas . Autores : Jorge Alejandro Quiroga *Cruz & Sergio David Cubillos Herrera Director : José*. 108. http://hdl.handle.net/11349/14634

RODRIGUEZ, N. (2018). Historia de la tecnología Blockchain – Infografía de línea de tiempo. *101blockchains*, *0*(0), 1–3.

Sharmaa, Y., & Prof. B. Balamurugan. (2020). Preserving the Privacy of Electronic Health Records using Blockchain. *ScienceDirect*, 173–180.

Shuyun Sh. (2020). Las aplicaciones de la cadena de bloqueo para garantizar la seguridad y la privacidad de sistemas de registros sanitarios electrónicos: Una encuesta. *Computers & Security*, 17–22.

Valiente, S. A. (2018). BLOCKCHAIN EN SALUD¿Quimera o realidad? *REVISTA DE LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA Y SALUD*.

Adilmou Jahid. (2018). tutorial-blockchain-python. https://github.com/

Lizcano, D. (2018). *Blockchain: posibilidades y aplicaciones al dominio de la medicina y los datos clínicos*. 5482. https://doi.org/10.3390/mol2net-04-0548

Jeet, R., & Singh Kang, S. (2020). Investigating the progress of human e-healthcare systems with understanding the necessity of using emerging blockchain technology. *Materials Today: Proceedings*, *xxxx*. https://doi.org/10.1016/j.matpr.2020.10.083

Sahebi, I. G., Masoomi, B., & Ghorbani, S. (2020). Expert oriented approach for analyzing the blockchain adoption barriers in humanitarian supply chain. *Technology in Society*, *63*(May), 101427. https://doi.org/10.1016/j.techsoc.2020.101427

Ul Hassan, M., Rehmani, M. H., & Chen, J. (2020). Differential privacy in blockchain technology: A futuristic approach. *Journal of Parallel and Distributed Computing*, *145*, 50–74. https://doi.org/10.1016/j.jpdc.2020.06.003

Pandey, P., & Litoriya, R. (2020). Implementing healthcare services on a large scale : Challenges and reme dies base d on blockchain technology. *Health Policy and Technology*, *9*(1), 69–78. https://doi.org/10.1016/j.hlpt.2020.01.004

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., Gupta, B., Lal, B., Misra, S., Prashant, P., Raman, R., Rana, N. P., Sharma, S. K., & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, *55*(July), 102211. https://doi.org/10.1016/j.ijinfomgt.2020.102211

Li, Z., Barenji, A. V., & Huang, G. Q. (2018). Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robotics and Computer-Integrated Manufacturing*, *54*(May), 133–144. https://doi.org/10.1016/j.rcim.2018.05.011

Kullig, N., Lämmel, P., & Tcholtchev, N. (2020). Prototype implementation and evaluation of a blockchain component on IoT devices. *Procedia Computer Science*, *175*, 379–386. https://doi.org/10.1016/j.procs.2020.07.054

Aggarwal, S., & Kumar, N. (2020). Blockchain 2.0: Smart contracts. In *Advances in Computers* (1st ed.). Elsevier Inc. https://doi.org/10.1016/bs.adcom.2020.08.015

Fu, X., Wang, H., & Shi, P. (2021). A survey of Blockchain consensus algorithms: mechanism, design and applications. *Science China Information Sciences*, *64*(2), 1–

15. https://doi.org/10.1007/s11432-019-2790-1