UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO DE INTEGRACIÓN CURRICULAR

previo a la obtención del Título de:

INGENIERA EN TECNOLOGÍAS
DE LA INFORMACIÓN

TEMA: "Vulnerabilidades existentes en técnicas tradicionales de almacenamientos de datos vs tecnologías emergentes como blockchain en entidades gubernamentales"

AUTOR

SAQUICELA TIGUA MITZI NOEMI

PROFESOR TUTOR:

ING. IVAN CORONEL, Msia

LA LIBERTAD – ECUADOR

2022

AGRADECIMIENTO

El camino de un estudiante universitario suele ser en cierto modo difícil, porque se aprenden nuevas cosas, aprendes a amar tu carrera, a darle un sentido profesional a tu vida, y estas son decisiones que marcan tu vida. A pesar de ser trabajoso contamos con el apoyo moral y emocional de nuestros padres, familia, amigos, profesores y a la UPSE. Y de la persona que nos apoyó para dar el último paso y el más importante, el tutor.

Les agradezco a mis padres, a mí papa Franklin y a mí mama Gloria por apoyarme, en cada decisión que tome en el transcurso de mi vida estudiantil. Y aunque uno de ellos ya no está conmigo, estoy segura de que el estaría orgulloso de mi. A mi familia que a pesar de estar lejos siempre me animaron a seguir estudiando y a no decaer en el transcurso.

Les agradezco a mis amigos que siempre tenían palabras de aliento para levantar el ánimo y decirme que lo iba a lograr.

Estoy sumamente agradecida por los profesores que conocí: Ing. Iván Coronel, Ing. Marjorie Coronel, Ing. Jaime Orozco, Ing. Gabriela Campuzano, Ing. Carlos Sánchez, Ing. Alicia Andrade, Ing. Shendry Rosero, Ing. Daniel Quirumbay, Ing. Omar Castellanos siempre tan dedicados a enseñar, a entender, a felicitar, a animar, a llamarnos la atención cuando se debía; pero estoy feliz de haberlos conocido, y de ellos me queda su enseñanza y en cierto modo su amistad.

En deuda con el Ing. Iván Coronel, no solo por ser un gran docente, también se encargó de guiarme siendo mi tutor, y asimismo se convirtió en un gran amigo. Finalmente, a la responsable de abrirme las puertas para poder estudiar, agradezco a la Universidad Estatal Península de Santa Elena, que, junto con sus autoridades, y trabajadores, hacen que el campus de enseñanza sea como un segundo hogar para cada uno de nosotros, porque de ella obtuvimos el conocimiento.

Mitzi Noemi Saquicela Tigua

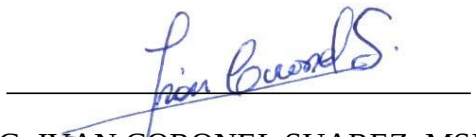
DEDICATORIA

Dedico este trabajo que realice con mucho esfuerzo y dedicación a mis padres a Franklin Saquicela y Gloria Tigua que me apoyaron desde el inicio de mi carrera estudiantil, a mi hermana Katherine que siempre estuvo conmigo.

Mitzi Noemi Saquicela Tigua

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de titulación denominado: **"Análisis de vulnerabilidades en técnicas tradicionales de almacenamiento vs tecnologías de blockchain en entidades gubernamentales. Caso de Estudio: Municipalidad de la Provincia de Santa Elena"**, elaborado por la estudiante **SAQUICELA TIGUA MITZI NOEMI**, de la carrera de **Tecnologías de la Información** de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo al estudiante para que inicie los trámites legales correspondientes.



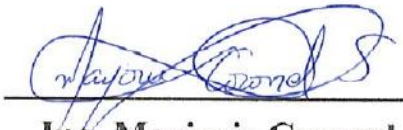
ING. IVAN CORONEL SUAREZ, MSIA.

TRIBUNAL DE GRADO

Ing. Jaime Orozco, Mgt.
DIRECTOR DE CARRERA

Lsi. Daniel Quirumbay, Msia
PROFESOR ESPECIALISTA

Ing. Iván Coronel, Msia
PROFESOR TUTOR



Ing. Marjorie Coronel, Mgt
DOCENTE GUÍA

RESUMEN

El presente trabajo investigativo pretende dar a conocer el uso de las tecnologías Blockchain o cadenas de bloque en el ámbito administrativo, refiriéndose a un Gobierno Autónomo Descentralizado Municipal de la Provincia de Santa Elena.

Las tecnologías blockchain forman parte de la "cuarta revolución", porque posee características únicas e innovadoras que permiten tener seguridad, transparencia, inmutabilidad, versatilidad, entre otros, al momento de almacenar información. Dejando atrás problemas de inseguridad relacionado a temas cibernéticos, como robo de información, fraude, hackeo de datos. Las cadenas de bloque permiten dejar a un lado la intervención de terceros y permite que la información sea "publica". A diferencia de las bases de datos tradicionales que tienden a tener fallos en los sistemas, son inseguras y por lo general, necesitan un tercero para realizar un correcto funcionamiento.

Parte de la investigación se centrará en explicar a breves y profundos rasgos el significado, la utilidad, el funcionamiento y las características de las bases de datos tradicionales vs las tecnologías blockchain.

Con la ayuda de las técnicas de recolección de datos se escogió el tipo de blockchain, en el caso del GAD municipal, es posible usar una cadena de bloque hibrida entre pública-privada, lo que permitirá la seguridad en los datos almacenados. Finalmente, se pretende realizar un ejemplo de cómo funcionan las cadenas de bloque, para ello se usarán herramientas relacionadas a la creación de bloques que formarán parte de la cadena final.

Palabras claves: Blockchain, cadenas de bloques, vulnerabilidades, bases de datos, administración pública, gobierno, contratos inteligentes, Remix IDE, solidity, Metamask.

ABSTRACT

This research work aims to present the use of Blockchain technologies in the administrative field, referring to a Municipal Decentralized Autonomous Government of the Province of Santa Elena.

Blockchain technologies are part of the "fourth revolution", because it has unique and innovative features that allow to have security, transparency, immutability, versatility, among others, when storing information. Leaving behind insecurity problems related to cyber issues, such as information theft, fraud, data hacking. Blockchains leave aside the intervention of third parties and allow the information to be "public". Unlike traditional databases, which tend to have system failures, they are insecure and generally require a third party to operate correctly.

Part of the research will focus on explaining in brief and in depth the meaning, usefulness, operation and characteristics of traditional databases vs. blockchain technologies.

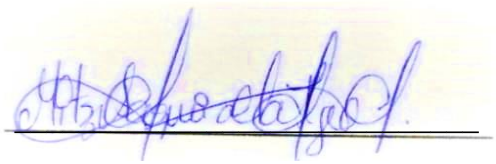
With the help of data collection techniques, the type of blockchain was chosen, in the case of the municipal GAD, it is possible to use a hybrid public-private blockchain, which will allow security in the stored data. Finally, it is intended to make an example of how blockchains work, for this purpose tools related to the creation of blocks that will be part of the final chain will be used

Keywords

Blockchain, vulnerabilities, databases, public administration, government, smart contracts, Remix IDE, solidity, Metamask.

DECLARACIÓN

El contenido del presente Trabajo de Graduación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena



SAQUICELA TIGUA MITZI NOEMI

TABLA DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

En la actualidad el mundo cada día avanza más tecnológicamente, y los problemas de seguridad informática son cada vez más sutiles, las personas a veces no conocen este tipo de problemas, y en el caso de entidades públicas y privadas, son atacadas con mayor frecuencia, porque en los datos está el poder. Teniendo en cuenta algunos ataques cibernéticos que han ocurrido en estas entidades se abre la duda de que si existe una tecnología capaz de respaldar la información de tal manera que sea confiable, integra y se encuentre disponible, no solo para la entidad sino también para las personas.

Uno de los aspectos más interesantes de esta investigación es poder conocer como las tecnologías de blockchain pueden erradicar la inseguridad, evitar corrupción dentro de las entidades públicas, aquellas que sufren ataques por ladrones cibernéticos, los robos más comunes son a través de ransomware, ingeniería social, inyección SQL, que atacan los servidores y bases de datos, para luego pedir recompensas o dinero a cambio de no publicar o hacer daño con la información obtenida.

El presente trabajo investigativo basado en comprender las tecnologías blockchain, además de sus funciones y características, también se toman en cuenta algunas de las bases de datos tradicionales, y pretende realizar un demo de cómo funcionan las cadenas de bloque tanto en una interfaz gráfica, como la explicación de un Smart contracts en back-end.

Este documento se encuentra segmentado en tres capítulos:

Capítulo I: dentro del contenido se encuentran: antecedentes, descripción del proyecto, objetivos, justificación, alcance, y metodologías implementadas en el trabajo investigativo, lo que demuestra que el uso de bases de datos tradicionales es peligroso sin las medidas de seguridad correctas, sin embargo, también se explica acerca de las tecnologías blockchain que han sido de utilidad en entidades públicas para emigrar información, almacenar y realizar la criptografía correspondiente.

Capitulo II: en este se podrá encontrar toda la información relacionada con el marco contextual, que explica las funcionalidades de un GAD Municipal, además de tener en cuentas algunas leyes ecuatorianas previo al desarrollo de la propuesta. También se encuentra el marco conceptual, donde se realizó un estudio bibliográfico de las

tecnologías blockchain, las bases de datos y sus relaciones. Finalmente se encuentra el marco teórico que especifica algunos de los trabajos relacionados con el tema directamente que ayudaron al estudiante a comprender mejor el uso de blockchain.

Capitulo III: este último capítulo cuenta con la información detallada de las cadenas de bloque, además de tener los cuadros comparativos que permitirán conocer porque Blockchain es una tecnología de "almacenamiento" mejor en temas administrativos y de seguridad informática

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1. ANTECEDENTES

Actualmente la información global se encuentra almacenada en algún dispositivo electrónico, sistema o programa, aunque todos los avances tecnológicos han sido muy útiles, también existen vulnerabilidades que impiden que los datos se encuentren almacenados de manera segura. [1] Estamos en una época digital en donde entidades gubernamentales, empresas públicas o privadas, hospitales, asociaciones o usuarios en general tienen almacenada su información en bases de datos y estas suelen ser vulneradas. ¿Por qué las bases de datos son de tanta importancia? Debido al papel fundamental que tienen al ser usadas como centro de almacenamiento de información de todo el mundo.

Se conoce que las principales amenazas a los servicios de almacenamiento son: inyecciones SQL, denegación de servicios, phishing, ingeniería social, malwares en general, ransomware, errores físicos, errores catastróficos, errores humanos que pasan inadvertidos para el usuario. [2] Las amenazas y las vulnerabilidades son aquellas que ponen en riesgo la integridad de la información; lo que provoca ataques masivos o consecutivos en la base de datos perpetrándola y provocando perdida de datos, perdida económicas y desconfianza en las personas.

Detrás de cada robo de información existen actores maliciosos o piratas informáticos que a menudo buscan rescates u otro tipo de beneficios económicos, y en muchas ocasiones estos ataques pueden ser efectuados con una serie de motivos, incluidos propósitos de activismo político, desestabilización de gobiernos, empresas, u organizaciones en general. [3]

Para saber que Ecuador también sufre ataques cibernéticos se hizo una investigación exploratoria en la web con la finalidad de dar a conocer qué tipo de ataques existen en

tiempo real. (Ver Anexo 1). Ubicado en el puesto 37 con incidencias de malwares y softwares maliciosos. (Ver Anexo 2). En el 2015 Ecuador fue atacado cibernéticamente lo que afecto a empresas privadas y públicas, saboteando procesos de contratación, pidiendo rescate por información, el robo de datos, suplantación de identidad en algunas redes sociales, etc. [4]

En Ecuador, para el año 2019, existió una falla informática que expuso información de casi toda la población, que para ese año superaba a los 17 millones de habitantes. La base de datos usada por la empresa ecuatoriana Novarest, mantenía un servidor sin seguridad, lo que permitía a cualquier persona acceder a ellos. El hallazgo se produjo luego de realizar un proyecto sobre mapeo web a gran escala, donde las direcciones y puertos IP, fueron escaneados y se encontraron vulnerabilidades; el servidor de dicha empresa se encontraba en Miami, una nube de información abierta con datos de ciudadanos incluyendo los de muchos fallecidos.

Los datos expuestos fueron: Nombres completos, genero, fecha de nacimiento, lugar de nacimiento, correo electrónico, dirección domiciliaria, número de teléfono de casa, trabajo y celular, estado civil, fecha de matrimonio, nivel de educación y hasta la fecha de fallecimiento. Conjuntamente también existía datos sensibles como estados de cuentas bancarias, saldo actual, dinero financiado, créditos, placa de auto, marca, modelo, y una lista de relaciones familiares, incluyendo información de casi 6.7 millones de niños. [5]

Otro ataque se dio en el año 2020, cuando Canon USA confirmo que se vio afectada por un ataque de ransomware, donde se robó información de empleados y de clientes entre los años del 2005 al 2020. Los actores maliciosos denominados MAZE tuvieron acceso a los servidores de archivos. Todo indica que el incidente ocurrió entre el 20 de julio al 6 de agosto del mismo año, cuando se emitió un aviso oficial, donde se explicó los problemas que venían sufriendo en el sistema que afectaba a múltiples aplicaciones, equipos, correos electrónicos y otros sistemas. Algunos de los datos correspondían a nombres, números de seguro social, información de nacimiento, numero de licencia de conducir, números de cuentas bancaria, firmas electrónicas de los empleados actuales y anteriores. La información en riesgo fue de 10 TB de datos privados y base de datos. [6]

Debido a las inseguridades que abordan a las bases de datos, surge una tecnología que cambia la manera en que la información es almacenada, se trata del Blockchain o cadenas de bloque. Las tecnologías blockchain permiten “acabar” con las inseguridades de las

técnicas tradicionales de almacenamiento, dejando a un lado la lentitud de los procesos, la desconfianza, la transparencia y elimina intermediarios; es decir su funcionalidad es directa. [7]

La Universidad Politécnica de Valencia desarrollo un estudio de "Blockchain aplicado al sector público", donde se dejó en claro los beneficios que tendría aplicar estas cadenas de bloque en sectores administrativos y en instituciones, pues deja a un lado la inseguridad de los datos e impide que un tercero intervenga, evitando la corrupción y aumentando la confianza de la ciudadanía en sus instituciones. [8]

Un artículo publicado el 2017 titulado "Aplicación de Tecnologías Blockchain en el gobierno de China"; analiza el marco, las dificultades y los desafíos de aplicar blockchain al gobierno electrónico en la actualidad, y analiza cómo la tecnología blockchain puede contribuir al desarrollo del gobierno electrónico y los servicios públicos en China. También toma en cuenta la ciberseguridad como base primordial para realizar los cambios. [9]

En Latinoamérica, el XXV Congreso Argentino de Ciencias de la Computación titulado "Blockchain y gobierno digital" menciona el auge de las tecnologías de blockchain respecto a seguridad, confiabilidad y transparencia de los datos. Y como esta tecnología ha sido una mejora en el gobierno. [10]

En Ecuador; después de la revisión bibliográfica se encontraron pocos temas enfocados o relacionados con tecnologías blockchain en el ámbito de almacenamiento; sin embargo, si existen otros tipos de investigaciones e implementaciones como se mencionan a continuación: En la Universidad de Guayaquil, se realizó una "Implementación de un prototipo de una red descentralizada blockchain para el voto electrónico en la Universidad de Guayaquil"; donde se da a conocer que las tecnologías blockchain permiten realizar las transacciones sin intermediarios, es decir, de una manera descentralizada y es precisamente esto lo que le da seguridad. Blockchain permite un gran número de posibilidades para su implementación y una de estas es el voto electrónico. [11]

Asimismo, un año después se realizó un "Análisis y diseño de un arquetipo para una solución Blockchain orientada a la seguridad de la información de aplicaciones en línea utilizadas en terapias médicas. Caso de aplicabilidad para el modelo de seguridad del diseño de la aplicación TEMONET." Donde propone que la información médica está segura y que este a disposición de terceros o que se vulnere los datos médicos. [12]

Gracias a las tecnologías blockchain se han encontrado solución a muchos problemas que parecían imposibles resolver, sobre todo resguardar la información, que se mantenga transparente y que no existan vulnerabilidades que la afecten. Debido a que es un tema de interés relacionado a la ciberseguridad, esta investigación pretende abarcar con las ventajas que mantienen las cadenas de bloque, realizando comparativas con algunas bases de datos relacionales y no relacionales, en cuestión del funcionamiento de las transacciones y seguridad. Al finalizar se quiere obtener un demo del funcionamiento de las cadenas de bloque, o una simulación de una base de datos distribuidas enfocada en tecnologías blockchain que permitirán asegurar la información mediante claves criptográficas, una red distribuida y un sistema de registro único. [13]

1.2. DESCRIPCIÓN DEL PROYECTO

Debido a que gran parte de la información que se encuentra almacenada es vulnerada, amenazada o existen riesgos de inseguridad, nace la idea de mejorar esta situación a través de la tecnología del blockchain o cadenas de suministro, que se reconocen por brindar seguridad y es una manera innovadora de respaldar los datos, además de poseer transparencia en todas sus acciones. Donde el libro de registros distribuidos tendrá acceso a la información, de manera segura, confiable, transparente, inmutable y sobre todo integra debido a las claves privadas criptográficamente que posee. [14]

El presente estudio se apegará a la metodología ADDIE, del cual se tomarán 4 etapas del modelo a aplicar. El análisis de toda la información, funcionalidad y características de las bases de datos relacionales y no relacionales, y acerca de las tecnologías blockchain; diseñar o proyectar acerca del tipo de blockchain, y cuáles son las bases de datos tradicionales que se pondrán a prueba, el desarrollo donde se acoplara toda la información encontrada acerca de las bases de datos más utilizadas y las cadenas de bloque en función buscando inicializar la simulación y evaluación final.

- **Análisis:**

Se realiza el levantamiento de la información, y se pone énfasis a descubrir, información relacionada de las bases de datos, además de realizar una investigación acerca de blockchain. Se busca a través de un estudio bibliográfico, cuáles son las vulnerabilidades que afectan a las bases de datos más utilizadas, estas pueden ser relacionales y no relacionales, en torno a entidades públicas, investigaciones realizadas, proyectos, entre otros, y se busca la diferencia de las cadenas de bloque en cuestión de seguridad y del funcionamiento, a su vez como están siendo utilizadas en un entorno público. Se realizará

cuadros comparativos entre las diferentes bases de datos que existen tomando puntos clave como: seguridad, consultas, integridad de los datos, consistencia de datos, complejidad, etc.

- **Diseño**

En este punto lo que se busca conseguir es reunir la información necesaria, para poder comenzar a desarrollar las cadenas de bloque en torno a la administración pública, por lo cual tendrá que escogerse un tipo de blockchain que sea útil, que se apegue al uso que se le dará. También se mostrarán los diferentes aplicativos que tiene el Blockchain en la actualidad. A su vez se buscarán las vulnerabilidades de los sistemas gestores de base de datos, con la finalidad de plantear en retrospectiva las fallas que se pueden dar, que pueden ser por errores humanos o por fallas físicas.

- **Desarrollo**

Una vez seleccionado el tipo de blockchain que se utilizara, se reunirá información adicional que permitan al investigador, hacer uso para comenzar con el desarrollo de las cadenas de bloque, que comprenden desde la creación del bloque génesis, pruebas de trabajo, nodos, las validaciones, claves criptográficas, y que plataforma o programa se usara. Se proyectará los errores más comunes que tienen las bases de datos, se realizara un cuadro comparando estos fallos, y cuál es la diferencia al Blockchain.

- **Simulación y Evaluación**

Finalmente, lo que se quiere lograr es la creación de una cadena de bloques distribuida y mostrar cómo funciona, cuáles son sus ventajas, y demás aplicaciones que tiene esta tecnología emergente. Se mostrarán los resultados de los fallos que tienen las bases de datos relacionales y no relacionales.

Para cumplir con todo lo mencionado anteriormente, se necesita utilizar herramientas que permitan crear cadenas de boque, y por lo tanto, también crear bases de datos, se hará uso de las siguientes herramientas:

- **Windows 10:** Windows es un sistema operativo, es decir, un programa de software que admite funciones básicas, como la administración de archivos y la ejecución de aplicaciones, y que usa dispositivos periféricos, como la impresora, entre otros. En el pasado, Windows podía considerarse como un software que

residía solo en tu dispositivo. Ahora con Windows 10, las partes importantes de Windows se basan en la nube e interactúan con los servicios en línea. [15]

- **Postman:** es una plataforma de API para crear y utilizar API. Postman simplifica cada paso del ciclo de vida y agiliza la colaboración. Almacena, repite y colabora fácilmente en torno a todos sus artefactos de API en una plataforma central que se utiliza en todos los equipos. [16]
- **Anaconda Navigator:** es un ambiente de trabajo para la ciencia de datos que permite hacer funcionar aplicaciones y administrar fácilmente distintos paquetes. Así, Anaconda Navigator puede buscar paquetes en Anaconda Cloud o en otros repositorios, y está disponible para ambientes Windows, macOS y Linux. [17]
- **Spyder:** el entorno de desarrollo científico de Python es un entorno de desarrollo integrado (IDE) gratuito que se incluye con Anaconda. Incluye funciones de edición, pruebas interactivas, depuración e introspección. [18]
- **Visual studio Code:** es un IDE completo para desarrolladores de .NET y C++ en Windows. Completamente equipado con una matriz de herramientas y características para elevar y mejorar todas las etapas del desarrollo de software. [19]
- **Node JS:** es un entorno de ejecución de Java Script orientado a eventos asíncronos, Node JS está diseñado para crear aplicaciones network escalables. [20]
- **Remix Ethereum:** permite desarrollar, implementar y administrar contratos inteligentes para Ethereum como blockchain. También se puede utilizar como plataforma de aprendizaje [21].
- **Truffle ganache:** sirve para activar una cadena de bloques Ethereum personal que puede usarse para ejecutar pruebas, ejecutar comandos e inspeccionar el estado mientras controla cómo funciona la cadena [22].
- **Metamask:** es una comunidad global de desarrolladores y diseñadore, es un software de Criptomoneda que es instalado como extensión de un navegador web [23].

El siguiente proyecto sigue la línea de investigación relacionada con temas de infraestructura y seguridad de las tecnologías de la información, tecnologías verdes, virtualización y computación en la nube, seguridad de la información, el Internet en las cosas a través de las redes de comunicación, sensores eléctricos y sistemas informáticos,

sistemas de información geográfica, gestión de seguridad de la información que permitan generar información indispensable para la toma de decisiones. Además, se relaciona con temas de gestión de desarrollo de software para tecnologías de gestión de base de datos, inteligencia de negocios (minería de datos) con la finalidad de dar soporte a las decisiones en tiempo real a las empresas. [24]

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Analizar la viabilidad de Blockchain como tecnologías emergentes enfocada a la seguridad de la información, a diferencia de las técnicas tradicionales de almacenamiento, a través de un estudio bibliográfico y un demo de cadenas de bloque, con la finalidad de documentar el trabajo como guía.

1.3.2. OBJETIVOS ESPECÍFICOS

- Examinar las metodologías tradicionales de almacenamiento, sus ventajas y desventajas, a través de una investigación previa
- Comparar las bases de datos relacionales y no relacionales, vs tecnologías blockchain, tomando en cuenta su funcionalidad y principales características
- Identificar ventajas de las tecnologías blockchain a través de un estudio bibliográfico.
- Construir un entorno con las herramientas necesarias con la finalidad de crear las cadenas de bloque.

1.4. JUSTIFICACIÓN

Las tecnologías blockchain tienen un papel fundamental en la cuarta revolución industrial; son reconocidas por ser seguras, confiables, dejar a un lado a los terceros, e inclusive se las conoce por la disponibilidad e integridad de sus datos. Blockchain permite a sus principales actores llevar registros compartidos e indelebles, con lo que reducen costes, disminuyen riesgos y se eliminan puntos centrales susceptibles a fallos. [25]

Algunas de las ventajas que tienen las tecnologías blockchain marcan un “antes” y “después”, en el ámbito de administración pública, según Heng Hou [9] en el artículo titulado “La aplicación de la tecnología Blockchain en el Gobierno electrónico en China”; menciona que mejora la calidad de los servicios gubernamentales, desarrolla el sistema, fortalece la credibilidad, promociona la integración. ¿Por qué las tecnologías blockchain son un punto clave a nivel informático y público? Debido a cuatro funcionalidades que

destacan: transparencia debido a que los datos se encuentra incorporados dentro de la red y por definición son públicos; incorruptibilidad al hecho que las cadenas de bloque son computacionalmente incorruptibles, pues informáticamente hablando tendría que modificar todas las copias o anular el objetivo; tiene un red de nodos que son inalterables en todo momento; y finalmente son descentralizados no existe ninguna entidad en la red que tenga control total de ella. [26]

También es necesario reconocer que el blockchain no solo existe para los bitcoins o las criptomonedas, este uso es solo "la punta del iceberg". Las cadenas de bloque son un registro único, consensuado y distribuido en varios nodos de una red. Seguros debido a que cada bloque tiene un lugar específico e inamovible dentro de la cadena; estas tecnologías permiten almacenar información que no se puede perder, modificar o eliminar; además está el hecho que cada nodo de la red utiliza certificados y firmas digitales para verificar la información validando las transacciones y tener autenticidad en los datos almacenados. [27]

Actualmente la mayor parte de la información de cada ciudad se encuentra almacenado en las bases de datos, y a pesar de que estamos en plena época de crecimiento tecnológico, todavía se usan sistemas de almacenamiento tradicional en muchos lugares, y al parecer esto no desaparecerá debido a la manera en que las personas, empresas u instituciones públicas o privadas están acostumbradas a hacer. [28] Es por esta razón que parte del presente trabajo será realizar una simulación de tecnologías blockchain basada en un modelo de información que intenta demostrar que la fuga de datos es casi nula, aunque es un nuevo concepto para muchos, las cadenas de bloque representan el futuro.

Con el estudio bibliográfico a desarrollar y el demo de las tecnologías blockchain se busca consolidar la información, lo cual permitirá conocer más acerca de las cadenas de suministro y como pueden implementarse en el sector público de nuestro país. Las instituciones públicas también son atacadas y en algunos casos la integridad de los datos es vulnerada; lo que puede provocar un daño permanente o un riesgo dentro de los sistemas de la institución

Las tecnologías blockchain son capaces de minimizar en gran porcentaje el robo de información. E inclusive permite la llevanza de bases de datos de forma descentralizada, «distribuida», sin necesidad, de contar siempre con una «autoridad central», o entidad poseedora de la información, que actúe como garante y como intermediaria. También

estas tecnologías están protegidas por una variedad de mecanismos, entre los que se incluyen técnicas avanzadas de criptografía y modelos de comportamiento y toma de decisiones matemáticos. [29]

Este caso de estudio tiene el propósito de realizar una investigación profunda acerca de tecnologías blockchain y bases de datos, con el fin de presentar cadenas de bloque. El presente trabajo investigativo contribuye a los objetivos del Plan de Creación de Oportunidades vigentes desde el 2021-2025 en [30]:

Directriz 1: Soporte territorial para la garantía de derechos

Lineamiento territorial A. Acceso equitativo a servicios y reducción de brechas territoriales.

A4. Fortalecer la conectividad y el acceso a las TIC como una vía para mejorar el acceso a otros servicios.

Objetivos del Eje Económico

Objetivo 5. Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social.

Política 5.5 Mejorar la conectividad digital y el acceso a nuevas tecnologías de la población.

Objetivos del Eje Seguridad Integral

Objetivo 10. Garantizar la Soberanía nacional, integridad territorial y seguridad del estado

Política 10.1 Fortalecer al Estado para mantener la confidencialidad, integridad y disponibilidad de la información frente a amenazas provenientes del ciberespacio y proteger su infraestructura crítica.

Objetivos del Eje Institucional

Objetivo 14. Fortalecer las capacidades del Estado con énfasis en la administración de justicia y eficiencia en los procesos de regulación y control, con independencia y autonomía.

Política 14.3 Fortalecer la implementación de las buenas prácticas regulatorias que garanticen la transparencia, eficiencia y competitividad del Estado

Las políticas y lineamientos del Plan Nacional de Desarrollo tienen la capacidad de brindar un equilibrio socioeconómico entre la ciudadanía. Aumentando la competitividad y este trabajo tiene la finalidad de promover la trasparencia en el ámbito informático. Ayudando a la protección de datos.

1.5. ALCANCE

Tomando como principal guía el objetivo general que menciona un análisis de viabilidad de Blockchain como tecnologías emergentes enfocada a la seguridad de la información, a diferencia de las técnicas tradicionales de almacenamiento, en el sector; se procede a realizar dicho objetivo; se realizara un estudio bibliográfico que permita conocer características, ventajas de dicha tecnología. Cabe recalcar que el alcance de este proyecto tiene la finalidad de demostrar los problemas de inseguridad que existen en los métodos de almacenamiento tradicional por lo cual parte de la investigación es teórica. Al finalizar el estudio bibliográfico también se pretende realizar un demo donde se migrarán datos hacia cadenas de suministro.

Fase de análisis

- Levantamiento de información
- Recopilación de información acerca de la situación actual respecto a las vulnerabilidades existentes en técnicas tradicionales de almacenamiento.
- Recopilación de datos acerca de las tecnologías emergentes como cadenas de bloque.
- Recopilación de información acerca de casos de estudio a nivel nacional, latinoamericano, internacional.

Fase de diseño

- Elección de herramientas necesarias para la creación de cadenas de bloque
- Elección de plataformas para el modelado de base de datos
- Establecimiento de riesgos y vulnerabilidades, en bases de datos relacionales y no relacionales.
- Ventajas de las cadenas de bloque en la administración pública.
- Indagar acerca de bases legales, en parte de administración pública.

Fase de desarrollo

- Desarrollo de blockchain, inicializando con el bloque “génesis”. Y desarrollo respecto a la cadena de bloque.
- Análisis comparativo de base de datos y blockchain

- Análisis comparativo de base de datos relacionales y no relacionales
- Estudio de trabajos ya propuestos, que permitan colaborar en el trabajo predispuesto.
- Vulnerabilidades de las bases de datos relacionales y no relacionales

Fase de simulación y evaluación

- Creación de bloques
- Creación de cadena de bloques
- Resultados obtenidos para la documentación.

Asimismo, se destaca que la indagación acerca de plataformas de blockchain dependen mucho del ámbito al cual se enfocan; la manera de funcionamiento y operación. Para finalizar se recopilará todo el conocimiento obtenido con el propósito de crear cadena de bloques.

1.6. METODOLOGÍA DEL PROYECTO

1.6.1. METODOLOGÍA DE LA INVESTIGACIÓN

La metodología de la investigación busca mostrar los elementos para la búsqueda, recolección e interpretación de la información lo cual se vuelve importante para realizar el siguiente proyecto. [31]

Aplicación de la metodología de la investigación diagnostica y la investigación exploratoria

Para el presente trabajo se realizará investigación diagnostica se refiere a la investigación que comprende la recolección de datos para probar hipótesis o responder a preguntas concernientes a la situación de estudio. [32]. Por esta razón la investigación diagnostica tiene la finalidad de conocer más acerca de las tecnologías blockchain y que funcionalidad tienen en el ámbito de sector público. Para saber también como tienen almacenado los datos, se toma en cuenta un GAD municipal donde se usarán métodos de recolección de datos, en este caso se usará la encuesta y el cuestionario con la finalidad de conocer cómo se encuentra estructurada la red de "almacenamiento".

A su vez también se desarrollará la metodología de investigación exploratoria que consiste en examinar un tema o problema de investigación poco estudiado, del cual se tienen dudas o no se ha abordado antes. [33]. Dada que es una investigación poco estudiada y no existen investigaciones claras referentes acerca de la ejecución en el ámbito gubernamental la implementación de tecnologías blockchain también se

desarrollara investigación exploratoria. Sé realizará un estudio bibliográfico y finalmente la etapa dos del proyecto constará con una pequeña simulación de una cadena de suministros sencilla.

1.6.2. Metodología de recolección de información

Las entrevistas y el cuestionario serán realizados dentro de las instalaciones del GAD municipal, y los resultados serán colocados en este documento para conocimiento; sin embargo, la información como datos personales de quienes respondan las preguntas se mantendrán de manera confidencial. Se llevará a cabo dentro de los horarios laborables, los martes y los viernes, tomando en cuenta el personal que accede al departamento de sistemas, si tienen capacitaciones o charlas acerca de nuevos métodos de seguridad o almacenamiento, solo por observación. Se considerará también si tienen centro de datos y como se maneja. Con el estudio se propone una variable cualitativa la cual tiene como prioridad comprobar que almacenar información a través de cadenas de bloque es más segura que guardar los datos en BD tradicionales.

1.6.3. Análisis de la Entrevista

Con el objetivo de conocer el trabajo que se realiza dentro del GAD municipal se realizó una entrevista al Coordinador del Departamento de Sistemas y Recursos Tecnológicos, y las respuestas fueron las siguientes:

Pregunta 1: ¿El GAD municipal ha sufrido un ataque cibernético o algún tipo de robo de la información?

Respuesta: no, en mi periodo no ha existido ninguno

Aunque la respuesta emitida por el entrevistado es un rotundo no, en medios de comunicación mencionan que si existen ataques relacionados con entidades gubernamentales, ya que la información de las provincias de la ciudadanía en particular se encuentran almacenadas en las instituciones. Por lo tanto, al comentar que en el periodo del actual administrador no ha existido ningún ataque, queda la duda si en periodos anteriores hubo ataques cibernéticos.

Pregunta 2: ¿El municipio se encuentra preparado en este momento para un ataque informático?

Respuesta: La prevención es una de las protecciones para un ataque informático el departamento técnico está en constante monitoreo de nuestra red informática junto al

cambio de claves periódicas. Utilización de VLAN para segmentar de manera lógica la red física. Además de contar con proxy y firewall para establecer canales de comunicación seguros y barreras de seguridad frente a las amenazas externas.

La seguridad cibernética dentro de la institución pública se puede decir que es "segura", ya que manejan firewalls , vlan, proxy que permiten tener canales seguros de comunicación, y son un obstáculo ante los hackers para atacar, aunque cabe destacar que si se expone situaciones como por ejemplo "ingeniería social", el personal del GAD desconoce todo lo referente al tema, por lo que la Municipalidad no cuenta con charlas o seminarios para capacitar a todo sus trabajadores en estos temas de seguridad cibernética.

Pregunta 3: ¿Cuentan con protocolos de seguridad informática?
Respuesta: En el área del Data Center si se cuenta con protocolos de seguridad tales como en los servidores las contraseñas se deben cambiar frecuentemente y alternar mayúsculas, minúsculas y números. Actualizar los sistemas Operativos, etc.

El administrador de la Municipalidad menciono que cuentan con protocolos cibernéticos que les permiten mantenerse en alerta ante cualquier ataque, sin embargo, los equipos del GAD no son cuentan con protocolos a seguir si existe algún desastre natural o error humano.

Pregunta 4: ¿De qué manera crean respaldos de la información (usan raid o backup)?

Respuesta: se realizan a través de backup

Las copias de seguridad se dan cada viernes al culminar la semana de trabajo, aunque los servidores de recuperación se encuentran en el mismo Data center que la Municipalidad tiene, por lo que nuevamente se recalca el punto de no tener medidas ante desastres naturales o situaciones externas de lo que tiene que ver con seguridad lógica.

Pregunta 5: ¿Quién puede acceder a su centro de datos? (en caso de contar con uno)

Respuesta: si se cuenta con un data center, solo accede el personal autorizado del Departamento de Sistemas y Recursos Tecnológicos.

La entrada al centro de datos no es custodiada por ningún personal de seguridad, todos los trabajadores del área de TIC´s puede ingresar sin necesidad de alguna tarjeta de identificación o llave maestra al ingresar a esta área. Cabe recalcar que el centro de datos se encuentra dentro del departamento que mantiene la puerta cerrada, pero deja entrar al personal de otras áreas.

Pregunta 6: ¿Qué base de datos usan actualmente?

Respuesta: en este momento se cuenta con Oracle 11G

La municipalidad solo usa el sistema de Oracle 11G, por motivos de que ya se había adquirido esta base de datos en anteriores administraciones y todo el personal estaba familiarizado con los procesos de Oracle 11G.

Pregunta 7: ¿Quiénes tienen acceso de a modificar, actualizar, o revisar las bases de datos?

Respuesta: solo el administrador de base de datos

Resulta que el administrador comparte responsabilidades con el resto del personal, por lo que los accesos a realizar cambios en las bases de datos son permitidos a todos los trabajadores de área, lo que prende una alerta ante cualquier ataque cibernético

Pregunta 8: ¿Tienen contraseñas las bases de datos?

Respuesta: si, solo el Administrador de Base de Datos la tiene.

Sin embargo, las contraseñas las conoce todo el personal debido a que están "capacitados", para realizar los cambios a través del terminal.

Pregunta 9: ¿Qué entiende por cadenas de bloque?

Respuesta: no he escuchado esa termino por lo tanto no se para que sirve

El desconocimiento de la tecnología Blockchain en funciones de almacenamiento resulta desconocida en todos sus aspectos o funciones.

Pregunta 10: ¿Ha escuchado acerca de las bases de datos distribuidas o del término Blockchain?

Respuesta: Desconozco el termino Blockchain, pero si he escuchado de las criptomonedas y bitcoin

Pregunta 11: ¿Entiende el termino SQL INYECTION?

Respuesta: claro que si, es un tipo de ataque dirigido a base de datos

Aunque existen un sinnúmero de vulnerabilidades hacia las bases de datos, el personal está familiarizado con el ataque de SQL Inyection, por lo que los temas relacionados contra los riesgos que corren las BD son conocidas.

Pregunta 12: ¿Conoce el termino DDOS?

Respuesta: Son ataques de denegación de servicio.

Pregunta 13: ¿Tienen un software de antivirus instalados en los pc de su departamento?

Respuesta: Si en equipos con sistema operativo Windows.

No existen sistemas operativos con Linux, o eso se dio a conocer por los empleados del municipio.

Pregunta 14: ¿Se puede acceder a la base de datos fuera del horario laboral o remotamente?

Respuesta: depende solo si es necesario

Resumen: a través de la técnica de recolección de información utilizada la entrevista se pudo obtener datos relacionados a cómo se encuentra la municipalidad en estudio, claramente el personal del departamento de recursos tecnológicos y sistemas mencionó que se encuentran preparados ante un ataque pero no han revisado si lo han sufrido anteriormente, que cuentan con protocolos de seguridad cibernética, aunque no cuentan con servidores fuera del departamento o servicios en la nube, ni seguridad al momento de ingresar al centro de datos, tienen conocimientos leves de lo que significan alguna de las vulnerabilidades que podrían sufrir las bases de datos; sin embargo no conocen acerca de la tecnología blockchain como una ayuda que los beneficiaría como entidad gubernamental.

Por lo que al final de la conversación con cada uno de ellos se explicó lo que las cadenas de bloques proporcionarían a la entidad gubernamental y cómo ayudarían a cumplir con los 3 pilares fundamentales de ciberseguridad; además de realizar otras preguntas en cuestión a la organización del departamento, y a cómo está dividido el sistema informático del edificio. hola a su vez se hizo una breve observación de cómo está dividido las oficinas y el centro de datos.

1.6.4. Análisis del Cuestionario

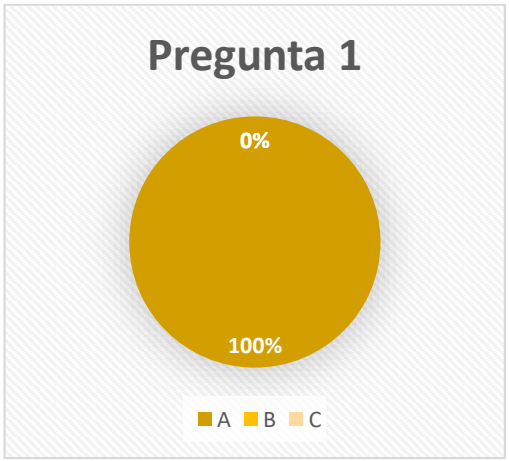
Con el objetivo de "Reconocer las necesidades y el objetivo a alcanzar, previo a la utilización de blockchain.", se realizó un cuestionario al personal del departamento de Sistemas y Recursos Tecnológicos, compuesto por seis personas, de las cuales tres de ellas respondieron; basándonos es un cuestionario presentado por el BID cuando se desea conocer si la opción de blockchain es necesaria se obtuvo la siguiente información

- ¿Necesita que todo el personal guarde, algún tipo de registro de información?

  A. Sí, todos los usuarios de la entidad involucrada generan información que necesita ser registrada.

  B. Sí, pero solo algunos usuarios generan información que se almacena

  C. No, solamente un grupo pequeño de la entidad genera información que se registra.



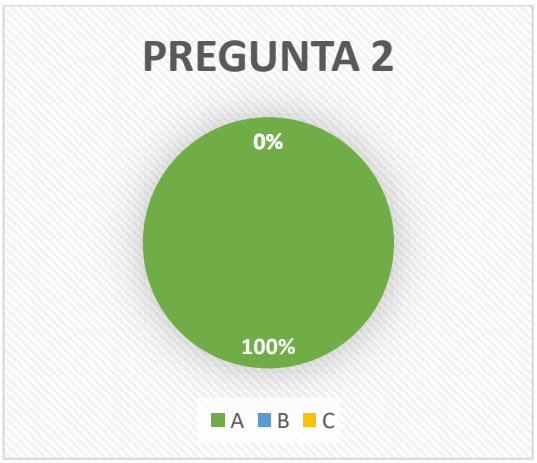
Todas escogieron la respuesta A.

- ¿Necesita que todo el personal tenga acceso al registro de la información?

  A. Sí, todos los usuarios de la entidad involucrada necesitan acceso a la información.

  B. Sí, pero solo algunos usuarios tienen acceso

  C. No, solamente un grupo pequeño de la entidad necesita acceso a la información.

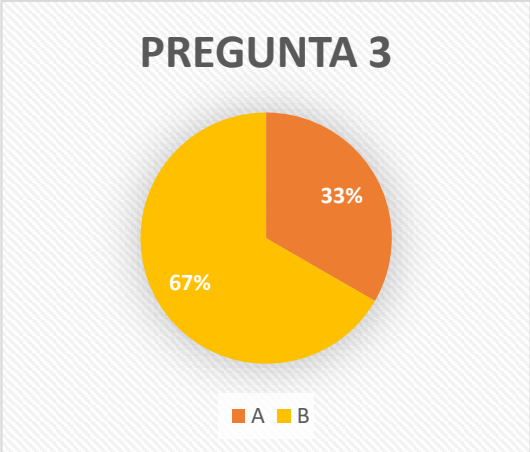


Mencionaron que todo el personal necesita acceso a la información, cabe recalcar que cada departamento tiene sus credenciales, y no tienen acceso a toda la información

- ¿Alguno de los involucrados tiene incentivos para intentar falsificar la información del registro para sus propios intereses?

  A. Sí.

  B. No



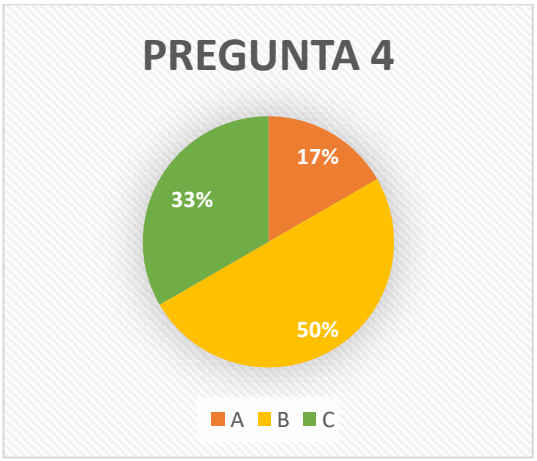
Cuatro personas respondieron que no existe nadie que intente falsificar la información, sin embargo, dos de ellos menciono que es posible la amenaza que se intente modificar la información para sacar provecho.

- ¿Necesitas validar el registro de nueva información en tiempo real o casi real?

  A. No, puedo esperar más de 10 minutos para validar un registro.

  B. No, pero solo puedo esperar hasta 10 minutos para validar un registro.

  C. Sí, necesito que la validación sea inmediata.



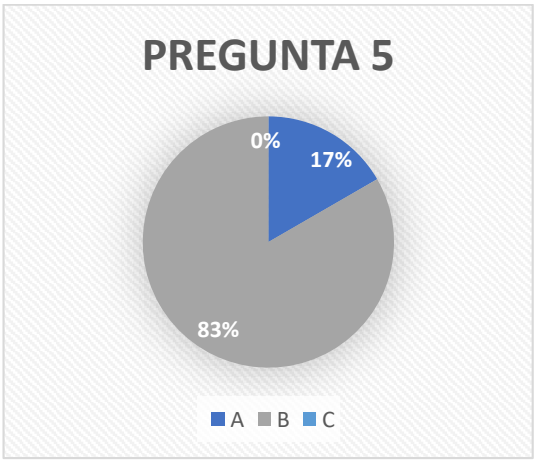
En este punto se pudo analizar las diferentes opiniones, que se dividían por el tema de la validación de datos en tiempo real. Cabe recalcar que la mayoría escogió la respuesta B, que decía que podían esperar 10 min para que los datos sean validados, y una persona menciono que no es necesario porque no se puede verificar toda la información al mismo tiempo, debido a que todas las áreas del GAD municipal se encuentran separadas.

- ¿Qué piensas de la existencia de una entidad central que valide/verifique toda la información para confirmar que es legítima y confiable? (EMPRESAS DUEÑAS DE SERVICIOS PRESTADOS)

  A. No la necesito.

  B. Idealmente no la quiero, pero no me molesta tenerla.

  C. Necesito y quiero una entidad así.



Realizaron un comentario de que "la anterior administración dejo el servicio con una entidad", pero ellos actualmente no la requerían, sin embargo, la seguían utilizando con la finalidad de evitar causar molestias a los demás departamentos.

- ¿Necesitas contar con registro histórico confiable de la información para auditarla o rastrearla?

  A. Sí.

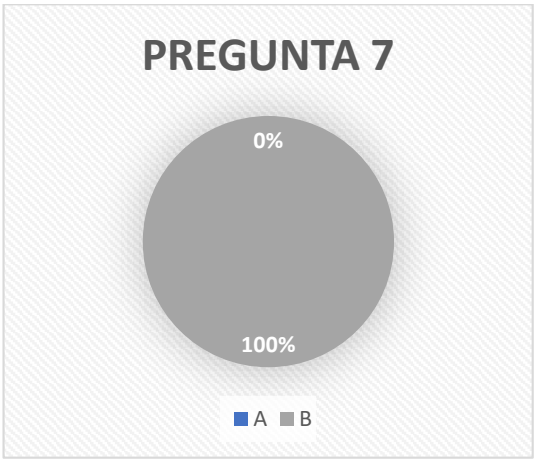
  B. No.

Para los empleadores del GAD Municipal es importante rastrear y tener un registro de la información, ya que se puede revisar los datos de manera local o de manera externa, ya que al ser una entidad gubernamental puede ser auditada en cualquier momento.

- ¿Necesitas que para acceder a la información registrada se siga algún proceso de validación o se consiga algún permiso? (claves)

  A. No.

  B. Sí.



Se necesitan validaciones porque así pueden tener seguridad en la información ingresada o que se revisa. Con el cuestionario se pretende escoger el tipo de plataforma blockchain a usar. En este caso las opciones más cercanas a la necesidad del GAD municipal corren del lado de blockchain hibrida/federada y privada, que tiene la finalidad de tener en parte una administración, sin embargo, los datos pueden ser de conocimiento público.

1.6.5. Metodología de desarrollo

El desarrollo del proyecto estará dividido en 4 fases. La primera fase está constituida por el análisis de la información, es decir, el levantamiento de la información como el primer paso a dar en el presente trabajo. Se buscará a través de un estudio bibliográfico, toda la información relacionada con lo que significa las bases de datos, y acerca de las tecnologías blockchain.

La segunda fase esta predispuesta por el diseño, lo que se quiere lograr es identificar los objetivos e ir desarrollando la documentación conforme a los mismos, además de indagar acerca de las vulnerabilidades que presentan las bases de datos tradicionales y dar un enfoque más claro a qué tipo de plataforma es la ideal para crear cadenas de bloque.

En la tercera fase se quiere desarrollar el contenido teórico y práctico, juntamente con la puesta en escena de la primera cadena de bloque o el bloque "génesis". Además de realizar cuadros comparativos. En la última fase de simulación y evaluación, se pondrá a prueba todo lo realizado anteriormente. Al finalizar se demostrará que las bases de datos

tradicionales no son 100% seguras, mientras que las cadenas de bloque son más eficaces, seguras y transparentes. Ayudaran a la administración pública, y a la protección de los datos de la ciudadanía en general. La imagen posterior muestra cada fase a tomarse en cuenta, vinculada a la metodología elegida como es ADDIE.

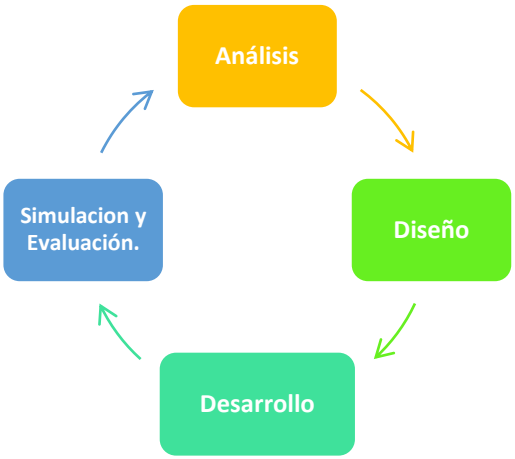


Figura 1: Metodología ADDIE. Elaboración propia.

Por el cual se obtiene las siguientes:

- Análisis y levantamiento de la información
- Diseño: identificar los objetivos e ir acorde a ellos para desarrollar la documentación
- Desarrollo del contenido teórico y practico
- Simulación y evaluación de Blockchain

CAPÍTULO II

2. LA PROPUESTA

2.1. MARCO CONTEXTUAL

A nivel mundial mantener la información resguardada de manera segura, ha ido cambiando conforme ha pasado el tiempo. A pesar de los cambios, la manera de almacenar los datos ha ido variando en el entorno de las existentes y nuevas bases de datos [34]. Sin embargo, la manera de proteger la información no es tan efectiva, debido a que las bases de datos presentan vulnerabilidades, y se vuelven blancos fáciles de atacar.

Muchos países han sido víctimas de estos ataques cibernéticos, que desequilibran a una nación completa, por ejemplo, las instituciones o gobiernos públicos son los blancos principales de estos robos. En Costa Rica, el 18 de abril del 2021, los sistemas institucionales del país fueron hackeados durante un mes el más afectado fue el Ministerio de Hacienda, donde los ciberdelincuentes usaron técnicas de ransomware para infectar y secuestrar la información de bases de datos en formato MSSQL, pidiendo $10 millones de dólares para cesar los ataques, y devolver los 900 GB de Bases de daros y 100GB de documentos internos [35].

Otro caso donde las bases de datos fueron expuestas a los ciberdelincuentes tomo partido en Alemania; en el 2017 este país fue víctima la filtración masiva de datos personales de políticos, periodistas y artistas, entre los datos mostrados en una red social fueron los números de tarjetas de crédito y direcciones de vivienda, se quiso sabotear la confianza de los ciudadanos [36]. Esta es la realidad de las entidades públicas, tener que vivir en la expectativa que pueden ser atacadas en cualquier momento, a pesar de poseer medidas de seguridad.

A diferencia de las técnicas tradicionales de almacenamiento, muchas instituciones van encaminándose hacia las cadenas de bloque donde la transparencia, confidencialidad, seguridad de ambas partes, y descentralización son las piezas fundamentales del cambio; además de poder establecerse como un modelo político y de gobernanza fomentando la creación de confianza social, eliminación de corrupción y prescindir de intermediarios [37].

A nivel nacional, no existen instituciones públicas que manejen sus datos en cadenas de bloque, más bien hacen uso de bases de datos como: Oracle, SQL Server, Mongo DB,

Cassandra, entre otras. Y en el medio donde se realiza esta investigación, la temática estará enfocada a analizar desde la perspectiva de una entidad gubernamental dentro de la Provincia de Santa Elena, analizando las técnicas de almacenamiento de Bases de datos y las mejores de Blockchain.

2.1.1. GOBIERNO AUTONOMO DESCENTRALIZADOS

Los Gobiernos Autónomos Descentralizados (GAD), son las instituciones que conforman la organización territorial del Estado Ecuatoriano y están regulados por la Constitución de la República del Ecuador (Art. 238-241) y el Código Orgánico de Organización Territorial, Autonomías y Descentralización (COOTAD); los GAD son instituciones descentralizadas que gozan de autonomía política, administrativa y financiera, y están regidos por los principios de solidaridad, subsidiariedad, equidad, interterritorial, integración y participación ciudadana [38].

Los gobiernos autónomos descentralizados son los encargados de promover el desarrollo sustentable y la dignidad de las personas, son capaces de implementar políticas públicas para la equidad y la inclusión social, además de permitir la participación ciudadana como ejercicio de los derechos plenos y la gestión democrática de la acción municipal, son los encargados de la ciudadanía en general [39].

Competencias de los GAD regionales

El Sistema Nacional de Competencias es un conjunto de instituciones, planes, políticas, programas y actividades vinculadas al ejercicio de las competencias.

- Planificar, con otras instituciones del sector público y actores de la sociedad, el desarrollo regional y formular los correspondientes planes de **ordenamiento territorial**, de manera articulada con la planificación nacional, provincial, cantonal y parroquial en el marco de la interculturalidad y plurinacionalidad y el respeto a la diversidad [40].
- Planificar, junto con otras instituciones del sector público y actores de la sociedad civil, el **desarrollo provincial y formular los planes de ordenamiento territorial**, en el ámbito de sus competencias, de manera articulada con la planificación nacional, regional, cantonal y parroquial, en el marco de la interculturalidad y plurinacionalidad y el respeto a la diversidad [40].

- Otorgar personalidad jurídica, registrar y controlar a las organizaciones sociales de carácter regional [40].
- Planificar el **desarrollo cantonal y formular los planes de ordenamiento territorial**, para regular el uso y ocupación del suelo urbano, en el marco de la interculturalidad y plurinacionalidad y el respeto a la diversidad [40].

El Gobierno Autónomo Descentralizado ubicado en la Provincia de Santa Elena, el cual es basado mi objeto de estudio en la presente investigación, posee características que lo diferencian de los demás GAD que existen dentro de Santa Elena. Su organización posee 5 niveles de macroprocesos, los cuales se dividen en:

- Macroproceso gobernante.
- Macroproceso habilitante asesoría.
- Macroproceso habilitante apoyo.
- Macroproceso agregadores de valor.
- Macroprocesos desconcentrados, empresas públicas y adscritos.

Nuestro estudio se enfocará en el tercer macroproceso, en Gestión Administrativa, específicamente en "Sistemas y Recursos Tecnológicos"; esta área se encarga de distribuir todo lo relacionado con tecnologías a la institución, además son los encargados de verificar que todos los sistemas relacionados con los servicios prestados se encuentren en línea y que funcionen de manera correcta. Entre algunos de los servicios prestados por la entidad pública que maneja información de la ciudadanía se encuentran: Catastros y Avalúos, Rentas, Contabilidad, Dirección Financiera, Coactiva, Tesorería, Terrenos, Dirección de Higiene, Justicia y Vigilancia, Talento Humano, Planificación, Construcción, Alcaldía, Mercados y Centros Comerciales.

La municipalidad en estudio posee una base de datos Oracle versión 11G, dentro del centro de datos se encuentran 9 servidores "propios" haciendo uso de una ip pública. Su backup se realiza cada viernes, como institución pública manejan servicios de seguridad externos, por ejemplo, hacen uso de cámaras de seguridad manejadas por el 911, no tienen servicios en la nube; su organigrama es de manera jerárquica y se encuentra dividido entre 5 personas, como se presenta en la figura 2, existe un encargado de coordinar el área, dos subdivisiones y cada una con dos funciones, para hacer funcionar la Municipalidad, esta posee planta baja, y dos pisos.

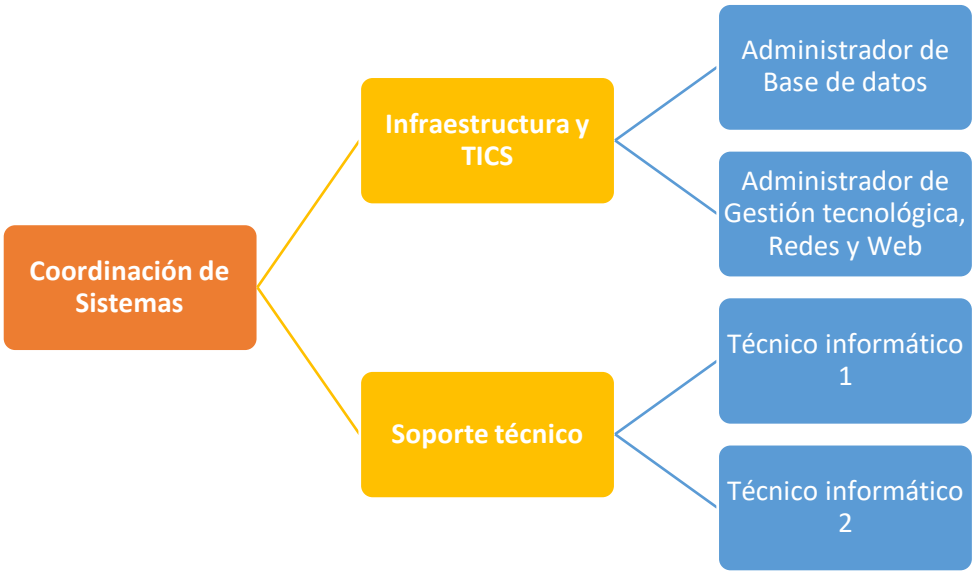


Figura 2: Estructura del departamento de Sistemas

MISIÓN

Promover el desarrollo humano sostenible, entregando a la comunidad servicios de calidad y calidez; con tal propósito desarrolla una gestión eficiente, transparente y participativa; contribuyendo de esta manera, al bienestar material y espiritual de la colectividad [38].

VISIÓN

El Gobierno Autónomo Descentralizado Municipal, con la participación de la ciudadanía y la planificación articulada con los distintos o iguales niveles de gobierno, contribuirá a construir un modelo de desarrollo humano sostenible y equitativo, que privilegia la consecución del buen vivir; constituyéndose de esta manera, en el motor del progreso cantonal y provincial. Su talento humano es solidario, altamente competitivo, honesto y comprometido con su institución y su cantón [38].

2.1.2. LEY DE PROTECCIÓN DE DATOS PERSONALES

El 10 de Mayo del 2021, se aprobó la ley Orgánica de Datos Personales, en la sesión 707 del pleno de la Asamblea Nacional. El objeto de la presente Ley es regular el ejercicio del derecho a la protección de datos personales, la autodeterminación informativa y demás derechos digitales en el tratamiento y flujo de datos personales, a través del desarrollo de principios; con la finalidad de procurar el adecuado tratamiento y flujo de los datos y que no exista vulneración de la seguridad de los dalos personales: Incidente de seguridad que

afecta la confidencialidad, disponibilidad o integridad de los datos personales, como por ejemplo la filtración [41].

El artículo 7 alude el tratamiento legítimo de datos personales; donde se recalca que estos solo podrán "usarse" con el consentimiento del titular, por algún tipo de interés público o en el ejercicio de poderes públicos conferidos al responsable, para la ejecución de medidas precontractuales a petición del titular, y para proteger intereses vitales, del interesado o de cualquier persona natural; finalmente se habla de satisfacer un interés legítimo del responsable o de un tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares [41].

El capítulo VI de la ley menciona acerca de la seguridad de los datos personales menciona: ***Artículo 37 Seguridad de datos personales:*** El responsable o encargado del tratamiento de datos personales. según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo con la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos [41].

El responsable o encargado deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales; el responsable o encargado del tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados, con la finalidad de resguardar y proteger los datos del ciudadano [41].

Entre otras medidas, se podrán incluir las siguientes:

1. Medidas de anonimización, seudonomización o cifrado de datos personales;
2. Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y,
3. Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, organizativa, y jurídica.
4. Los responsables y encargados del tratamiento de datos personales podrán acogerse a estándares internacionales para una adecuada gestión de riesgos

enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

Artículo 38. Medidas de seguridad en el ámbito del sector público: El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza. vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción, o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de los datos personales [41].

La aplicación de la "Ley Orgánica de datos Personales" no solo incluye empresas privadas o públicas; también abarca según el artículo 255 de la Constitución de la Republica del Ecuador a los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoras y de Transparencia y Control social; asimismo se apegan a la ley las entidades que integran el régimen autónomo descentralizado, los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado. [41]

Artículo 47: Obligaciones del responsable y encargado del tratamiento de datos personales. Se menciona 15 aspectos que se deben tomar en cuenta para el tratamiento de los datos personales, entre los que se resaltan:

- Tratar los datos personales en estricto apego a los principios y derechos desarrollados en la "Ley de Protección de Datos Personales", reglamentos, directrices, lineamientos y regulaciones emitidas por la autoridad competente.
- Implementar políticas de protección de datos personales afines del tratamiento de datos personales en cada caso particular.
- Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas.
- Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad a lo dispuesto en la presenta Ley, en su reglamento, en

directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales.

Cada aspecto se debe cumplir para que se cumplan las obligaciones y el tratamiento de los datos personales, en lo que sea aplicable, de acuerdo con la ley vigente en el Ecuador, desde el 26 de mayo del 2021, sin embargo cabe recalcar que existe un plazo de 2 años, hasta el 202, para que las empresas públicas o privadas, tomen medidas que impidan ser sancionados o multados por el mal tratamiento de los datos personales, una vez transcurrido ese tiempo la Ley Orgánica de Protección de Datos Personales entrará en vigencia en su máximo esplendor, por lo cual el proyecto será analizado con esta ley. [41].

2.1.3. CÓDIGO ORGANICO PENAL INTEGRAL

El código orgánico penal integral o más conocido como COIP, es una ley donde se aplican todos los principios provenientes de la Constitución de la República del Ecuador, en particular se aplica a los principios de tutela judicial efectiva y debida diligencia a fin de garantizar la reparación integral para las víctimas y la prevención de la reincidencia y de la impunidad [42]. Se quiere evitar cualquier tipo de manipulación, modificación o mal uso de los permisos prestados por la entidad pública.

En la sección novena titulada DELITOS CONTRA EL DERECHO A LA PROPIEDAD, el Artículo 190 referente a la **Apropiación fraudulenta por medios electrónicos** menciona que: *"La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años";* esta ley no solo es emitida contra personas individualmente, también es admisible a entidades [42].

Además de condenar el mal uso de infraestructura, programas, equipos, bases de datos o etiquetas que admitan en un cambio, reprogramación o alteración de la información, la sanción será de pena privativa de libertad de uno a tres años. En el pleno la sección tercera, **Delitos contra la seguridad de los activos de los sistemas de información y**

comunicación, el articulo 229 indica acerca de la Revelación ilegal de datos para beneficios de terceros, será condenado a pena privativa de uno a tres años, esto incluye la revelación de datos registrados en medios como: ficheros, archivos, bases de datos, o enviados a través de sistemas electrónicos, informáticos, telemáticos [42].

El artículo 230 hace referencia a la Interceptación ilegal de datos, donde alude a interceptar, escuchar, desviar, grabar u observar en cualquier forma un dato informático, asimismo cualquier persona que diseñe, desarrolle, venda, ejecute o envíe mensajes con información confidencial, será sancionada con pena privativa de libertad de tres a cinco años [42].

2.1.4. ÁMBITO DE ESTUDIO

Dentro de la investigación presentada en el trabajo, se hace una recolección exploratoria de teorías referentes a las vulnerabilidades existentes en técnicas tradicionales de almacenamiento de datos y las diferencias que tienen las tecnologías Blockchain. En el cual se seguirá un orden de estudio, después de la investigación realizada se expondrá lo analizado acerca de Bases de Datos relacionales y no relacionales, asimismo se explicará el uso del Blockchain y sus beneficios.

Una vez culminada la parte investigativa, se comenzará a desarrollar la propuesta de una simulación de cadenas de bloque, además de explicar su funcionamiento y algunas de sus aplicaciones, que es una temática innovadora de almacenamiento y seguridad informática, que tiene la finalidad de cumplir con los tres principios: Confidencialidad, Integridad y Disponibilidad de la información. Todo esto se llevará a cabo con el tema de una Municipalidad de la Provincia de Santa Elena, que posee varios servicios.

2.2. MARCO CONCEPTUAL

La investigación previa acerca de las bases de datos y de lo que se conoce de blockchain permitirá, indagar a fondo los temas que son importantes para nuestro estudio, por lo tanto, el estudio bibliográfico es fundamental. Se quiere adquirir la mayor cantidad de información pertinente que apoye nuestro estudio.

2.2.1. BASES DE DATOS

El concepto de base de datos ya es conocido en el entorno que nos envuelve, esta investigación es para conocer las diferencias de las bases de datos relacionales y no relacionales, asimismo, el tipo de base de datos que existen, cuáles son las

vulnerabilidades que estas presentan, todo esto se basara en bases de datos más conocidas en el medio público y privado.

TIPOS DE BASE DE DATOS

Existen varios tipos de base de datos, de acuerdo con el uso que se le va a dar en dicha área. Se pueden dividir según:

- ✓ **La variabilidad de los datos almacenados**

Existen 2 tipos de variabilidad de BD primero son las **bases de datos estáticas** son aquellas que primordialmente son de lectura, se usan para almacenar datos históricos, que pueden ser usados después de cierto tiempo, ayudan a la toma de decisiones. Segundo se conoce las **bases de datos dinámicas** son las más utilizadas ya que permite la modificación de los datos, permitiendo operaciones como actualización, además permite la adición de información [43].

- ✓ **El contenido**

En este tipo se encuentran también base de datos a texto completo: estas son aquellas que almacenan datos de fuentes primarias por eso se dividen en numéricas (Contienen datos numéricos como el nombre lo indica, por ejemplo, datos de censos o indicadores cuantitativos) y mixtas (En este se combinan los datos, por ejemplo, informes económicos, datos geoeconómicos, encuestas, etc.); y base de datos bibliográficas, que se usan mayormente en registrar información de publicaciones o de artículos científicos, de manera ordenada, se convierte en "contenedor de datos", y suelen usarse para información que proviene de las ciencias de la vida o médicas [43].

- ✓ **Base de datos jerárquicas**

Esta base de datos se asemeja a la estructura de un árbol, cada enlace es anidado con el fin de conservar los datos organizados en un orden particular en un mismo nivel de lista, los beneficios de usar este tipo de BD corresponden a las relaciones uno a uno que poseen, siendo fáciles de entender, a su vez permiten ver las modificaciones que se realizan [44].

- ✓ **Base de datos relacional**

Es conocida por ser una herramienta potente que no solo almacena la información también permite el acceso a ella, las bases de datos relacionales son organizadas en forma de tablas esta división permite que la información sea accesible además de poder añadir datos sin

reorganizar las tablas; una tabla puede tener muchos registros y cada registro puede tener muchos campos [44].

- ✓ **Base de datos orientada a objetos**

Es una base de datos que consta de objetos utilizados en la programación orientada a objetos. Los objetos similares se agrupan en una clase y cada objeto de una clase particular se llama su instancia. Las clases permiten que un programador defina datos que no están incluidos en el programa. Aunque se conocen más tipos, en este estudio se han tomado las más relevantes y las más usadas [44].

SISTEMAS GESTORES DE BASE DE DATOS

Un sistema gestor de base de datos o SGDB, es también conocido como DBMS (Data Base Management System) es una colección de datos relacionados entre sí, de manera que se encuentran estructurados y organizados, y un conjunto de programas que acceden y gestionan estos datos, en estos sistemas de gestión de archivos, la definición de los datos se encuentra codificada dentro de los programas de aplicación en lugar de almacenarse de forma independiente, y además el control del acceso y la manipulación de los datos viene impuesto por los programas de aplicación [45].

Los sistemas gestores de bases de datos se crearon debido a los inconvenientes como fallos humanos, que representaban la redundancia e inconsistencia de los datos, una dependencia de los datos física – lógica, dificultad para el acceso concurrente, dependencia de la estructuras de archivos con lenguaje, problemas de seguridad en integridad de los datos; por lo que los SGBD se encargan de la creación, gestión y administración de las bases de datos, además de que son las encargadas de aprobar el manejo y escoger la estructura de almacenamiento, lo que permite realizar búsquedas de información de manera eficiente [45].

2.2.2. CLASIFICACIÓN

Los sistemas gestores de bases de datos se dividen según la forma en la que se administra los datos:

- Relacionales (SQL)
- No relacionales (NoSQL)

En este estudio se investigará acerca de bases de datos tanto relacionales como no relacionales como son: MySQL, PostgreSQL, SQL Server, MongoDB, Redis, Cassandra.

- **RELACIONALES**

Este modelo se basa en establecer relaciones o vínculos entre los datos. Y los gestores de base de datos relacionales son las más usadas hoy en día para administrar la información.

MySQL: esta herramienta es de gran versatilidad muchas organizaciones la utilizan entre ellas mencionan a Facebook, Adobe, Alcatel, entra otras, ahorran tiempo y dinero ya que impulsan sus sitios web de alto volumen; algunos de los beneficios son gran facilidad de uso y rendimiento, fácil instalación y configuración, soporte multiplataforma y soporte SSL, una de sus desventajas es la escalabilidad [46].

Figura 3: Logo de MySQL

PostgreSQL: es un potente sistema de base de datos, que se ha ganado una buena reputación debido a la fiabilidad, solidez de funciones y un buen rendimiento. Esta herramienta viene con muchas características que permiten a los desarrolladores crear aplicaciones, proteger hasta cierto punto la integridad de los datos, tienen un entorno tolerante a fallas, es gratuito y de código abierto.; aunque también cuenta con una desventaja que es la lentitud para la administración de base de datos pequeñas, debido a que esta más enfocada a gestionar grandes volúmenes de información [47].

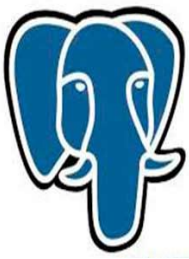


Figura 4: Logo de Postgre SQL

SQL Server: pertenece a la compañía de Microsoft, posee distintas herramientas. Tienen como principal característica una alta disponibilidad ya que permiten un gran tiempo de actividad y conmutación veloz.; esta desarrollado como un server que permite dar servicio a otras aplicaciones, algunas de sus características son: permiten soporte de transacciones, poseen escalabilidad, estabilidad, soporte a procedimientos almacenados, usan comandos de DDL y DML, permiten administrar datos en de otros servidores, basada en transact-SQL; aunque una desventaja podría ser el precio de la herramienta que se desea usar [48].

Figura 5: Logo de Sql Server

- **NO RELACIONALES**

Las bases de datos NoSQL están desarrolladas o diseñadas para modelos de datos específicos, tienen esquemas flexibles para crear aplicaciones modernas, no requieren de estructura de datos fija; son conocidas por ser fáciles de desarrollar, su funcionalidad y el rendimiento a escala que posee. NoSQL utilizan una variedad de modelos de datos para acceder y administrar datos [49].

Mongo DB: es una base de datos distribuida, basada en documentos y de uso general desarrollada para aplicaciones modernas; posee características como: potente lenguaje de consulta que permite filtrar y ordenar por cualquier campo independientemente del como este incrustado en un documento, está orientado a ficheros que almacena ficheros JSON, es open source, escalabilidad de forma horizontal, su desventaja es que no es muy adecuada para transacciones complejas. [50].

Figura 6: Logo de MongoDB

Redis: almacén de estructura de datos en memoria de código abierto (con licencia BSD), que se utiliza como base de datos, caché y agente de mensajes, Redis proporciona estructuras de datos como cadenas, hashes, listas, conjuntos, conjuntos ordenados con consultas de rango, mapas de bits, ,índices geoespaciales y flujo; su principal uso es para almacenar en memoria cache y administrar sesiones, sus características son atomicidad, persistencia, simplicidad, multiplataforma y velocidad [51].

Figura 7: Logo de REDIS

Cassandra: Apache Cassandra es una base de datos distribuida NoSQL de código abierto, la escalabilidad lineal y la tolerancia a fallas comprobada en hardware básico o infraestructura en la nube la convierten en la plataforma perfecta para datos de misión crítica [52].

Figura 8: Logo de Cassandra

2.2.3. SEGURIDAD EN BASES DE DATOS

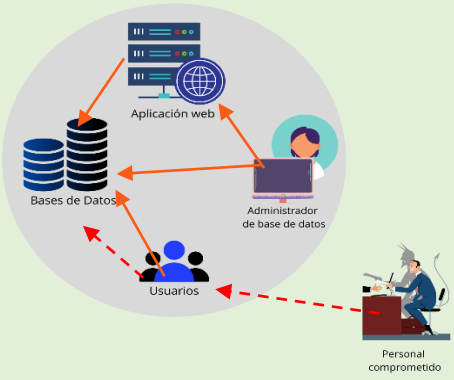
Las bases de datos en la actualidad se han convertido en una de las herramientas más usadas, con el fin de almacenar información que es utilizada a diario. Desde datos

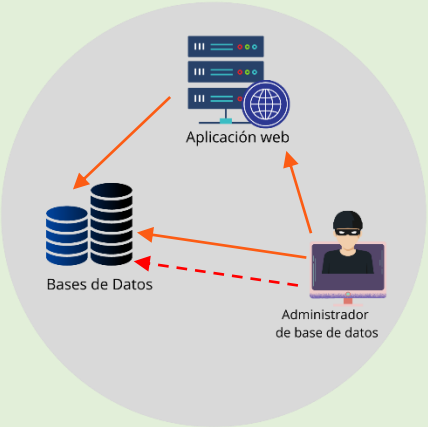
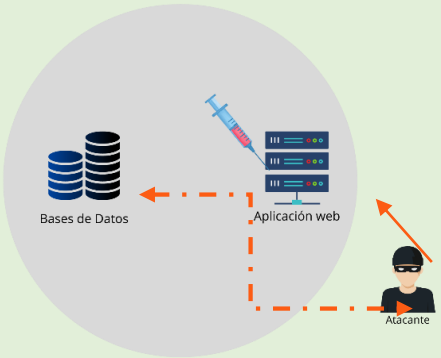
bancarios, médicos, educativos, de la población, gubernamentales, entre otros; están siendo guardados, por lo que podría argumentar que son una pieza clave al momento de querer irrumpir la seguridad y atacar, con la única finalidad obtener la mayor información y sacarle provecho de mala manera [53].

Y a pesar de que se desea erradicar que los datos sean liberados de manera no legal, o que se modifiquen, por lo que conlleva a robo de información no siempre es posible, en muchas ocasiones existen tipos de amenazas que pueden dividirse en dos: accidentales (sin intención de causar daño) o intencionales (causan daño) [54]. Debido a esto suele surgir la cuestión de la seguridad informática que se relaciona con proteger los datos de accesos no autorizados y evitar posible corrupción, la seguridad de los datos incluye lo que tiene que ver con encriptación de datos, tokenización, gestión de contraseñas para resguardar las aplicaciones o herramientas que use dicha organización [55].

2.2.4. VULNERABILIDADES GENERALES DE LAS BASES DE DATOS

El creciente uso de tecnologías en el siglo XXI ha conllevado que existan amenazas que intentan poner en peligro los datos o recursos que se encuentran almacenados dentro de las organizaciones y entidades, sean estas de carácter público, privado o aquellas que son sin fines de lucro [56]. En la Tabla 1, se muestran algunas vulnerabilidades de manera general que suelen ser usadas para infiltrarse en las bases de datos y hurtar información, haciendo uso de algunos inseguridades o desperfectos en las configuraciones de las BD

AMENAZA	*DESCRIPCIÓN*	*DETALLE*
Uso excesivo de privilegios innecesarios	Este tipo de amenaza ocurre cuando se otorgan privilegios excesivos a un usuario, creando un riesgo innecesario, se suele dar cuando no existe un control de privilegios por roles [57].	 *Figura 9: Un delincuente comprometió el dispositivo de un empleado y utiliza los privilegios excesivos que posee para acceder a la base de datos*

Abuso de privilegios	Ocurre cuando el personal que posee acceso a la base de datos abusa de este privilegio para robar o sustraer información sin autorización [57].	 *Figura 10: Un DBA o administrador de base de datos, hace uso de sus privilegios para hurtar información accediendo de manera ilegal, superando los permisos de la aplicación.*
Inyección por SQL	Las secuencias son inyectadas a través de la base de datos, almacenes con datos críticos, que no forman parte del SQL programado, teniendo acceso y dejando a los datos en estado crítico [57].	 *Figura 11: Un atacante hace uso de Inyection SQL, para acceder de manera maliciosa a la base de datos, y robar información.*
Auditorías superficiales	Por auditorias débiles, causadas por procesos internos insuficientes o vacíos, se da cuando no existe el monitoreo adecuado de las anomalías de seguridad,	 *Figura 12: Se dan cuando no existen procesos internos*

	cumplimiento y recopilación, la auditoría no contiene los detalles apropiados de las actividades de las bases de datos que representan un riesgo organizacional [57].	*suficientes o están vacíos, a su vez también se da por desconocimiento.*
Exposición de los medios de almacenamiento	Suelen darse por medio de backup insegura, también por no auditar y monitorizar las actividades de acceso de bajo nivel por parte de los administradores [57].	 *Figura 13: Existe una amenaza constante, esta se da cuando los medios de almacenamiento no son seguros, o quedan expuestos a otras personas, no siempre las backup son eficientes ante este peligro.*
Manipulación de datos o explotación de BD vulnerables	Existen puntos débiles en las BD, cuando no se han aplicado parches, o todavía mantienen cuentas y parámetros de configuración predeterminada. La exposición a manipular estos datos suele ser muy alta, debido a que	 *Figura 14: existen vulnerabilidades que un ladrón cibernético puede usar para modificar o hurtar información que proviene de una base de dato*

	si la empresa que brinda el servicio de base de datos no brinda seguridad la institución queda desprotegida [58].	

Tabla 1: Amenazas i/o vulnerabilidades generales de las Bases de Datos

Esas son algunas de las vulnerabilidades generales que existen dentro de las técnicas tradicionales de almacenamiento, para conocer más se realizó una investigación de las amenazas específicas que posee cada base de dato a estudiar.

2.2.5. VULNERABILIDADES ESPECÍFICAS DE LAS BASES DE DATOS

Para el siguiente trabajo se han recabado vulnerabilidades específicas de tres bases de datos relacionales: MySQL, Postgre SQL, SQL Server y tres bases de datos no relacionales como son Mongo DB, Redis y Apache Cassandra. Cada una de ellas poseen vulnerabilidades o amenazas, estas serán analizadas desde la página oficial de CVE. CVE o las "Vulnerabilidades y exposiciones comunes"; sirve para identificar, definir y catalogar las vulnerabilidades de seguridad cibernética divulgadas públicamente; hasta la actualidad aproximadamente hay 180,291 registros se ve accesibles a través de descargas o búsqueda por internet [59].

En la Tabla 2 se puede evidenciar cuales son los peligros que poseen las bases de datos relacionales.

BASES DE DATOS RELACIONALES	
Bases de datos	***Vulnerabilidades específicas***
MySQL	✓ ***CVE-2022-31026***: Trilogy es una biblioteca cliente para MySQL. Al autenticarse, un servidor malicioso podría devolver un paquete de autenticación especialmente diseñado, haciendo que el cliente lea y devuelva hasta 12 bytes de datos de una variable no inicializada en la memoria de la pila. Los usuarios de la trilogy gem deberían actualizar a la versión 2.1.1. Este problema puede evitarse conectándose únicamente a servidores de confianza [60] ✓ ***CVE-2022-21490:*** Vulnerabilidad en el producto MySQL Cluster de Oracle MySQL (componente: Cluster: General). Las versiones afectadas

	son 7.4.35 y anteriores, 7.5.25 y anteriores, 7.6.21 y anteriores y 8.0.28 y anteriores. La vulnerabilidad difícil de explotar permite a un atacante con altos privilegios con acceso al segmento de comunicación física conectado al hardware donde se ejecuta el MySQL Cluster comprometer el MySQL Cluster. Los ataques exitosos requieren la interacción humana de una persona que no sea el atacante. Los ataques exitosos de esta vulnerabilidad pueden resultar en la toma de control de MySQL Cluster [61] ✓ ***CVE-2021-42662***: Existe una vulnerabilidad de Cross Site Scripting (XSS) almacenada en el sistema de reservas de eventos online Sourcecodester en PHP/MySQL a través del parámetro Holiday reason. Un atacante puede aprovechar esta vulnerabilidad para ejecutar comandos JavaScript en nombre de los navegantes del servidor web, lo que puede conducir al robo de cookies y más [62]. ✓ ***CVE-2022-21460:*** Vulnerabilidad en el producto MySQL Server de Oracle MySQL (componente: Server: Logging). Las versiones afectadas son la 5.7.37 y anteriores y la 8.0.28 y anteriores. La vulnerabilidad difícil de explotar permite a un atacante con altos privilegios con acceso a la red a través de múltiples protocolos comprometer MySQL Server. Los ataques exitosos de esta vulnerabilidad pueden dar como resultado el acceso no autorizado a datos críticos o el acceso completo a todos los datos accesibles de MySQL Server [63].
Postgre SQL	✓ ***CVE-2013-0255:*** PostgreSQL 9.2.x antes de 9.2.3, 9.1.x antes de 9.1.8, 9.0.x antes de 9.0.12, 8.4.x antes de 8.4.16 y 8.3.x antes de 8.3.23 no declara correctamente la función enum_recv en backend/utils/adt/enum. c, lo que hace que se invoque con argumentos incorrectos y permite a los usuarios remotos autenticados provocar una denegación de servicio (caída del servidor) o leer memoria sensible del proceso a través de un comando SQL elaborado, lo que desencadena un error de índice de matriz y una lectura fuera de límites [64]. ✓ ***CVE-2009-4136***: PostgreSQL 7.4.x antes de 7.4.27, 8.0.x antes de 8.0.23, 8.1.x antes de 8.1.19, 8.2.x antes de 8.2.15, 8.3.x antes de 8.3.9 y 8.4.x antes de 8.4. 2 no gestiona correctamente el estado local de la sesión durante la ejecución de una función de índice por parte de un superusuario de la base de datos, lo que permite a los usuarios remotos autentificados obtener privilegios a través de una tabla con funciones de índice

	manipuladas, como se demuestra en las funciones que modifican (1) search_path o (2) una sentencia preparada, un problema relacionado con CVE-2007-6600 y CVE-2009-3230 [65]. ✓ ***CVE-2009-4034:*** PostgreSQL 7.4.x antes de 7.4.27, 8.0.x antes de 8.0.23, 8.1.x antes de 8.1.19, 8.2.x antes de 8.2.15, 8.3.x antes de 8.3.9, y 8.4.x antes de 8.4.2 no maneja correctamente un carácter '\0' en un nombre de dominio en el campo de Nombre Común (CN) del sujeto de un certificado X.509 lo que (1) permite a los atacantes de tipo man-in-the-middle falsificar servidores PostgreSQL basados en SSL mediante un certificado de servidor falsificado emitido por una Autoridad de Certificación legítima, y (2) permite a los atacantes remotos eludir las restricciones de nombre de host de cliente previstas mediante un certificado de cliente falsificado emitido por una Autoridad de Certificación legítima, un problema relacionado con CVE-2009-2408 [66]. ✓ ***CVE-2009-3231***: El componente del servidor central en PostgreSQL 8.3 antes de 8.3.8 y 8.2 antes de 8.2.14, cuando se utiliza la autenticación LDAP con enlaces anónimos, permite a los atacantes remotos eludir la autenticación a través de una contraseña vacía [67].
SQL Server	✓ ***CVE-2022-30335:*** Bonanza Wealth Management System (BWM) 7.3.2 permite la inyección SQL a través del formulario de inicio de sesión. Los usuarios que suministran a la aplicación una carga útil de inyección SQL en el cuadro de texto Nombre de usuario podrían recoger todas las contraseñas en formato cifrado del componente Microsoft SQL Server [68]. ✓ ***CVE-2021-38159:*** En ciertas versiones de Progress MOVEit Transfer anteriores a la 2021.0.4 (también conocida como 13.0.4), la inyección SQL en la aplicación web de MOVEit Transfer podría permitir a un atacante remoto no autenticado obtener acceso a la base de datos. Dependiendo del motor de base de datos que se utilice (MySQL, Microsoft SQL Server o Azure SQL), un atacante podría ser capaz de inferir información sobre la estructura y el contenido de la base de datos, o ejecutar sentencias SQL que alteren o eliminen elementos de la base de datos, a través de cadenas crafteadas enviadas a tipos de transacciones únicas de MOVEit Transfer [69]. ✓ ***CVE-2021-25275***: La plataforma Orion de SolarWinds antes de 2020.2.4, tal y como la utilizan varios productos de SolarWinds, instala y utiliza un

	backend de SQL Server, y almacena las credenciales de la base de datos para acceder a este backend en un archivo legible por usuarios sin privilegios. Como resultado, cualquier usuario que tenga acceso al sistema de archivos puede leer los detalles de inicio de sesión de la base de datos desde ese archivo, incluyendo el nombre de inicio de sesión y su contraseña asociada. A continuación, las credenciales pueden utilizarse para obtener el acceso del propietario de la base de datos a SWNetPerfMon.DB. Esto da acceso a los datos recogidos por las aplicaciones de SolarWinds, y conduce al acceso de administrador a las aplicaciones insertando o cambiando los datos de autenticación almacenados en la tabla Accounts de la base de datos [70]. ✓ ***CVE-2020-1455:*** Existe una vulnerabilidad de denegación de servicio cuando Microsoft SQL Server Management Studio (SSMS) maneja incorrectamente los archivos, también conocida como 'Microsoft SQL Server Management Studio Denial of Service Vulnerability' [71].

Tabla 2: Vulnerabilidades específicas de Bases de Datos Relacionales.

En la Tabla 3 encontrará información básica de las amenazas de las bases de datos no relacionales:

BASES DE DATOS NO RELACIONALES	
Bases de datos	***Vulnerabilidades específicas***
Mongo DB	✓ CVE-2022-24272: Un usuario autenticado puede provocar una aserción invariante durante el envío de comandos debido a una validación incorrecta en la base de datos $external; esto puede dar lugar a una denegación de servicio mongod o a la caída del servidor. Este problema afecta a: MongoDB Inc. versiones del servidor MongoDB v5.0, anteriores a la v5.0.6 inclusive [72]. ✓ CVE-2021-32040: Puede ser posible tener una canalización de agregación extremadamente larga junto con una etapa/operador específico y causar un desbordamiento de pila debido al tamaño de los marcos de pila utilizados por esa etapa, si un atacante pudiera provocar que se produjera tal agregación, podría bloquear maliciosamente MongoDB en un ataque DoS; esta vulnerabilidad afecta a las versiones de MongoDB anteriores a la 5.0.4, 4.4.11, 4.2.16 [73]. ✓ CVE-2021-32039: Los usuarios con acceso a archivos adecuado pueden acceder a las credenciales de usuario sin cifrar guardadas por MongoDB Extension para VS Code en un archivo binario, estas credenciales pueden

	ser utilizadas por atacantes maliciosos para realizar acciones no autorizadas; esta vulnerabilidad afecta a todas las extensiones de MongoDB para VS Code, incluidas y anteriores a la versión 0.7.0, [74]. ✓ CVE-2021-20334: Un tercero malicioso con acceso local a la máquina Windows donde está instalado MongoDB Compass puede ejecutar software arbitrario con los privilegios del usuario que ejecuta MongoDB Compass. Este problema afecta a: MongoDB Inc. MongoDB Compass 1.x versión 1.3.0 en Windows y versiones posteriores; Versiones 1.x anteriores a 1.25.0 en Windows [75].
Redis	✓ CVE-2022-0543: Se descubrió que redis, una base de datos clave-valor persistente, debido a un problema de empaquetado, es propensa a un escape de espacio aislado de Lua (específico de Debian), lo que podría resultar en la ejecución remota de código [76]. ✓ CVE-2021-33026: La extensión Flask-Caching hasta 1.10.1 para Flask se basa en Pickle para la serialización, lo que puede conducir a la ejecución remota de código o a la escalada de privilegios locales, si un atacante obtiene acceso al almacenamiento en caché (por ejemplo, sistema de archivos, Memcached, Redis, etc.), puede construir una carga útil manipulada, envenenar el caché y ejecutar código de Python [77]. ✓ CVE-2021-31649: En aplicaciones que usan jfinal 4.9.08 y versiones anteriores, existe una vulnerabilidad de deserialización cuando se usa redis, puede ser vulnerable a la ejecución remota de código [78]. ✓ CVE-2021-29469: Node-redis es un cliente de Node.js Redis. Antes de la versión 3.1.1, cuando un cliente está en modo de monitoreo, la expresión regular que se usa para detectar mensajes de monitoreo podría causar un retroceso exponencial en algunas cadenas. Este problema podría conducir a una denegación de servicio [79].
Apache Cassandra	✓ CVE-2021-44521: Al ejecutar Apache Cassandra con la siguiente configuración: enable_user_defined_functions: true enable_scripted_user_defined_functions: true enable_user_defined_functions_threads: false, es posible que un atacante ejecute código arbitrario en el host, el atacante necesitaría tener suficientes permisos para crear funciones definidas por el usuario en el clúster para poder explotar esto [80]. ✓ CVE-2021-40525: La implementación de Apache James ManagedSieve junto con el almacenamiento de archivos para scripts de tamiz es

vulnerable al cruce de rutas, lo que permite leer y escribir cualquier archivo [81].

- ✓ CVE-2020-13946: es posible que un atacante local sin acceso al proceso de Apache Cassandra o a los archivos de configuración manipule el registro RMI para realizar un ataque man-in-the-middle y capturar los nombres de usuario y las contraseñas utilizadas para acceder a la interfaz JMX, el atacante puede usar estas credenciales para acceder a la interfaz JMX y realizar operaciones no autorizadas, los usuarios también deben conocer CVE-2019-2684, una vulnerabilidad de JRE que permite explotar este problema de forma remota [82].
- ✓ CVE-2019-16869: Netty antes de 4.1.42.Final maneja mal los espacios en blanco antes de los dos puntos en los encabezados HTTP (como una línea "Codificación de transferencia: fragmentada"), lo que conduce al contrabando de solicitudes HTTP [83].

Tabla 3: Vulnerabilidades de Bases de datos No Relacionales

INCIDENTES DE SEGURIDAD

En un entorno mundial, en Estados Unidos, la Administración Nacional de Aeronáutica y el Espacio más conocida como NASA, fue víctima de un incidente de seguridad en Abril del 2018, el atacante logro robar información relacionada con una misión a Marte; afectando al Laboratorio de Propulsión a Reacción JPL, esta brecha permaneció sin ser detectada por 10 meses, el robo fue de unos 500 MB de datos, todo esto se hizo con la ayuda de un Raspberry PI conectado sin autorización a la red de JPL sin autorización [84].

En Latinoamérica, el Departamento Administrativo Nacional de Estadísticas DANE, de Colombia fue atacado cibernéticamente el 9 de Noviembre del 2021, el ataque no solo fue de extracción de información, sino que el atacante logro modificar y eliminar varios datos de la institución, según fuentes secundarias el robo de información fue de 130 TB; afectando por varios días la página oficial, 5500 funcionarios se vieron afectados, se afirmó que 420 servidores fueron infiltrados; finalmente el/los atacantes pedían dinero a cambio de la devolución de la información comprometida, este ataque fue enfocado a hacer daño material a la entidad pública [85].

En Ecuador, a principios de Febrero de 2021, Banco Pichincha sufrió un ataque informático, que afecto parte de los servicios prestados e inclusive puso en duda la integridad de la información de los clientes, dejando su sistema fuera de servicio

completamente, lo que incluía su portal web, los cajeros automáticos y su banca en línea; probablemente se debió a un ataque de ransomware por parte de la agrupación "Hotarus Corp" y estos confirmaron haber sustraído datos de clientes de la institución financiera [86].

Casi al mismo tiempo la misma agrupación ataco el Ministerio de Trabajo y de Finanzas, en Junio del 2021; donde implementó una cepa de ransomware basada en php para cifrar un sitio que alojaba un curso en línea, los autores del delito publicaron en un TXT o archivo de texto datos relacionados a 6632 nombres de inicio de sesión y claves de usuario; además de información referente: correos electrónicos, datos de empleados, contrato, etc [87].

Por otra parte, el miércoles 14 de Julio del 2021, la Corporación Nacional de Telecomunicaciones CNT, fue víctima de un ataque externo de ransomware EXX, que inhabilito el sistema informático, por lo que servicios como: facturación, activaciones, entre otras se vieron afectadas. Por lo que el Gobierno anuncio que la información encontrada en las bases de daros de las empresas públicas se centralizarían, con el fin de brindarles una "mejor protección"; el ataque ransomware no solo afecto las bases de datos, también vulnero instancias como servicios web, el robo de información según fuentes secundarias alcanzo los 11 GB, en parte fue descuido de la propia empresa al no poseer la seguridad informática necesaria para evitar o mitigar dichos ataques [88].

2.2.6. BLOCKCHAIN

Blockchain es un tipo de Tecnología Ledger Distribuida (DTL). Un DTL son datos que se encuentran replicados, compartidos y sincronizados entre diferentes sitios, instituciones o países, los DTL no tienen un administrador Central. Los blockchain están conectados a bloques anteriores por un algoritmo criptográfico que se conoce como "hash", formando una cadena de bloques [89].

Aunque las cadenas de bloque no son recientes, su aplicación a distintos campos es cada vez mayor. Desde áreas económicas, medicas, educativas, e incluso gubernamentales se pueden apegar a esta tecnología y mejorar en su funcionamiento [89].

El blockchain se puede dividir en diferentes partes (Ver Figura 15) como: la base de datos distribuida, el bloque de transacciones, el nonce, los nodos y el algoritmo de encriptación. Cada parte juega un papel importante al momento de almacenar, compartir o conocer la información que contiene [10].

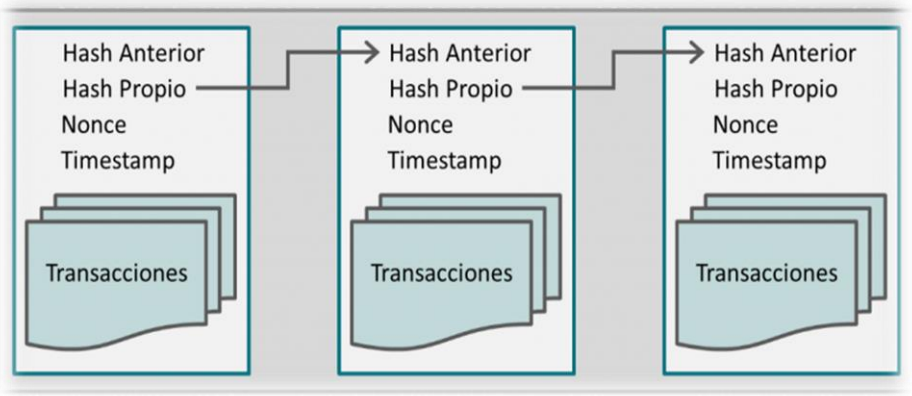


Figura 15: Cadena de Bloque. Fuente: WeLiveSecurity

Cada blockchain tiene una estructura, un funcionamiento, características propias, a la vez también depende que tipo de red se necesita al momento de aplicarla, cuáles son sus limitaciones y beneficios al apegarse a las cadenas de bloque y como ayudan en el área gubernamental conocer acerca de esta tecnología [27].

También se conoce como una base de datos que es casi imposible de hackear debido a que debe atacar a todos los nodos de la red para causar daño, esta propiedad está basada en las redes de almacenamiento y comunicación peer-to-peer (p2p), en la Figura 16 se muestra como son las estructuras del blockchain [90].

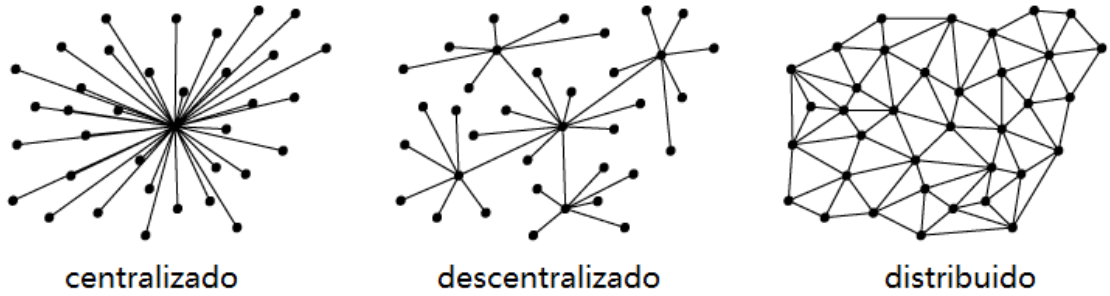


Figura 16: Tipos de Blockchain(estructura/esquema). Fuente: Estratega Financiera

TIPO DE ESTRUCTURA Y CARACTERÍSTICAS DEL BLOCKCHAIN

Blockchain posee tres tipos de estructura estas se conocen como públicas, privadas e hibridas:

Públicas: no existen restricciones para la lectura de datos ni para la realización de operaciones por parte de los usuarios, es abierta y cualquiera puede participar en ella [10].

Privadas: en este tipo de estructura la lectura de datos y las operaciones están limitadas a participantes determinados, los usuarios deben tener permiso de "administrador" para poder usarla [10].

Híbridas/Federadas: este tipo de estructura combina la pública y la privada. Siendo una buena opción ya que se usan las mejores soluciones de ambas, existe un número determinado de organizaciones, entidades o compañías que se encargan de administrar la red y mantener las copias del registro sincronizadas, el acceso a la red se hace mediante una interfaz web que los administradores ponen a disposición del usuario brindando, al mismo tiempo, un acceso controlado y libertad [10].

Por lo tanto, se puede usar cualquier tipo de estructura dependiendo de lo que se desee hacer y a que entidad u organización este dirigida [10]

Aunque según un artículo titulado "Blockchain: la revolución industrial de Internet"; menciona que se pueden definir entre centralizadas, descentralizadas y pseudoanónimas.

Centralizadas: cualquier persona sin ser usuario puede acceder y revisar o consultar las transacciones [91].

Descentralizadas: cuando no existe un usuario que tenga más poder que otro en la red; es decir todos los nodos son iguales entre sí [91].

Pseudoanónimas: cuando los propietarios de las transacciones son "anónimos" hasta cierto punto, pero sus direcciones son rastreables debido a carácter público [91].

Como todo tipo de tecnología, blockchain también posee características que la hacen sobresalir de las demás. Se conoce que las blockchain presentan características como:

Seguridad: se puede describir que una blockchain es segura, ya que hace uso de la criptografía, proporcionando seguridad sobre la información que se encuentra almacenada en las cadenas de bloque y en muchos casos distribuida en los nodos de la red; su uso depende mucho de tener a disposición un conjunto de claves asimétricas validad para poder operar, aunque no siempre se usa el mismo formato, toda transacción es firmada por el emisor; teniendo una clave pública que permite verificar que la información no ha sido modificada [92].

Otro parte de seguridad que tienen las cadenas de bloque se refiere al uso de hash que generan identificadores únicos para el contenido de cada bloque; permitiendo interconectarlos, e identificar si existe una alteración, la seguridad radica en la capacidad que poseen los nodos de la red en detectar algún cambio de los datos rechazando el bloque o la transacción [92].

Trazabilidad: esta característica hace que el blockchain sea auditable, porque permite recorrer la cadena de bloque y trazar todo los movimientos u operaciones que se realizado en determinada dirección, también permite retroceder en la cadena y revisar las transacciones; en blockchain todas las transacciones consolidadas se guardan en la cadena de bloques, por lo que es posible conocer las operaciones que se han realizado usando un explorador de blockchain [92].

Privacidad: esta característica se encuentra en el blockchain público, donde las direcciones de las cadenas de bloque no están vinculadas a las personas que las controlan. Para poder usar un blockchain público si es necesario que se disponga de claves públicas y privadas que permiten controlar la cadena de bloque, además, esta característica no está disponible en todas las distribuciones, ya que, en algunos casos, para poder operar sobre una red blockchain se requiere una identificación previa [92].

Transparencia: se consigue publicando las reglas que definen el funcionamiento del blockchain. Depende también del tipo de estructura que se esté usando, por lo general las cadenas de bloque de ámbito privadas tienen un bajo nivel de transparencia debido a que no se tiene acceso a los datos o es casi nulo, porque dependen de un administrador. [10] Se logra la transparencia cuando el código de software es hecho público y se puede operar la cadena de manera normal [92].

Confianza: sin intermediarios la tecnología base de los blockchain es el DTL, es decir las cadenas de bloque están hecha para dos personas que no confían entre sí y no quieren la intervención de un tercero [92]. Cada característica tiene su función y papel en el funcionamiento de las estructuras del blockchain. [92]

BENEFICIOS DEL USO DE BLOCKCHAIN

Cuando hablamos de beneficios de blockchain es proporcionar varias ventajas al usuario. Algunos de los beneficios más importantes son: durabilidad, transparencia, inmutabilidad, integridad del proceso [93].

Durabilidad: Las redes descentralizadas eliminan los puntos únicos de falla en comparación con los sistemas centralizados. Esta distribución del riesgo entre sus nodos hace que las cadenas de bloques sean mucho más duraderas que los sistemas centralizados y son más adecuadas para disuadir los accesos maliciosos [93].

Transparencia: Cada nodo de la red mantiene una copia idéntica de una cadena de bloques, lo que permite auditar e inspeccionar los conjuntos de datos en tiempo real. Este nivel de transparencia hace que las actividades y operaciones de la red sean muy visibles, lo que reduce la necesidad de confianza [93].

Integridad del proceso: Los protocolos de código abierto distribuidos se ejecutan por naturaleza exactamente como están escritos en el código. Los usuarios pueden estar seguros de que las acciones descritas en el protocolo se ejecutan de forma correcta y oportuna sin necesidad de intervención humana [94].

Inmutabilidad: Los datos que se almacenan en una blockchain pública distribuida son prácticamente inmutables debido a la necesidad de validación por otros nodos y trazabilidad de cambios. Esto permite a los usuarios operar con el mayor grado de confianza en que la cadena de datos no se modifica y es precisa [94].

Longevidad: Los dispositivos, servicios y aplicaciones que descargan su funcionalidad crítica de procesamiento de transacciones a una cadena de bloques pública que es independiente del fabricante del dispositivo, proveedor de servicios o desarrollador de aplicaciones, pueden infundir confianza en los consumidores y usuarios de que el dispositivo, servicio o aplicación continuará funcionando [94].

Fiabilidad y disponibilidad: Una cadena de bloques bien distribuida con un alto nivel de redundancia puede considerarse altamente confiable porque la

falla de cualquier nodo o grupo de nodos en particular no compromete las capacidades de procesamiento de transacciones de la cadena de bloques [94]. Aunque blockchain tiene beneficios, también posee limitaciones debido a la infraestructura de TI que necesitan las organizaciones, también se habla acerca de las actualizaciones constantes de tecnología en base de sistemas manuales o automatizados como etiquetas simples y RFID, que se deben adquirir para mantener los perfiles digitales en nivel alto y tecnológicos.

Para poder generar cadenas de bloque a grado industrial debe realizarse una investigación exhaustiva con la a finalidad de cumplir los requisitos para tener blockchain. Otra de las limitaciones podría darse debido a que blockchain no es totalmente legal en los países, por lo que no puede ser regularizado. También muchas veces entender las cadenas de bloque suelen ser confusas, debe considerarse el costo por transacción o la acción que se quiera realizar [95].

APLICACIONES DEL BLOCKCHAIN

En la actualidad la mayoría de las personas u organizaciones han escuchado hablar acerca del blockchain, por las criptomonedas, o dinero digital. Existen distintos campos o áreas que los usan [96] Por ejemplo, se puede usar para:

a. **Almacenamiento distribuido en la nube:**

En lugar de hacer uso de los servicios centralizados como Google Drive, Amazon o Dropbox, las cadenas de bloque ofrecen servicios P2P (peer to peer), no necesitan un sistema centralizado debido a que los datos quedan almacenados por múltiples miembros de la red [96]. Además, el sistema descentralizado que manejan las cadenas de bloque permite que la información se encuentre más segura, sea más económico y los datos permanecerán disponibles en su totalidad [97].

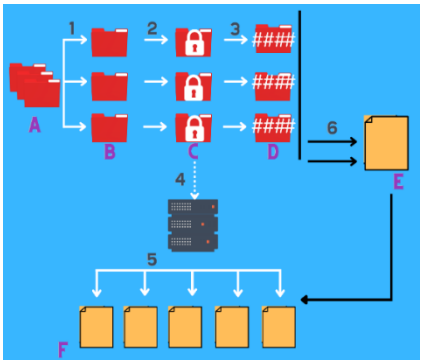


Figura 17: Basada en Blockchain Institute. Elaboración propia

En la Figura 17 se explica como funcionaría un almacenamiento descentralizado basado en blockchain.

1. Los datos (A) se dividen en varias partes (B).
2. Cada parte dividida se encripta (C) con la clave pública del usuario que almacenara el archivo.
3. Se genera un hash único (D) para cada fragmento.
4. Las partes que ya poseen un hash (C) se distribuyen a los nodos para el almacenamiento.
5. Las partes cifradas se replican en nodos pares, cada uno comparte una copia del libro mayor común (F).
6. Finalmente, los hashes se registran en la cadena de bloque (E) para cualquier referencia durante la recuperación.

b. Gestión de identidades:

En este punto las cadenas de bloque permiten crear una identidad única digital que hasta cierto punto es difícil de manipular, con un hash diferente al cada bloque, se estima que esta gestión de identidad podría cambias los usuarios y contraseñas en línea [96]. Una gestión de identidad a través de blockchain permitiría tener un mayor control y propiedad de los datos, se busca beneficiar a los "consumidores", y adquirir más confianza [98].

Figura 18: Gestión de identidades. Fuente: DPLNEWS

c. Ejecución automática de contratos

Ethereum es una herramienta que incluye la posibilidad de crear "contratos inteligentes o Smart contracts", se trata de programas que recogen los términos de un contrato entre las partes y las almacenan en las cadenas de bloque, con la única diferencia que se autoejecutan cuando se cumplen condiciones específicas [96].

Por lo general, se utilizan para automatizar la ejecución de un acuerdo o contrato en el que todos los participantes puedan enterarse de los resultados de manera inmediata sin la intermediación de un tercero y la pérdida de tiempo, los contratos inteligentes funcionan de manera simple siguiendo declaraciones como: "if/when…then…", que se escriben dentro de la cadena de bloques, por ejemplo los Smart contracts pueden usarse en la liberación de fondos económicos a las partes correspondientes, el registro de un automóvil, el envío de notificaciones, emisión de multa, entre otros [99].

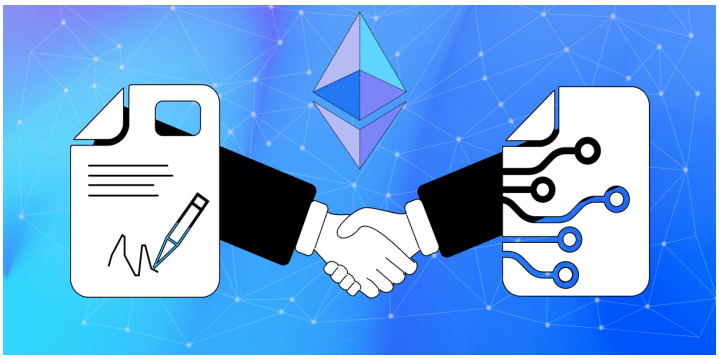


Figura 19: Smart contracts, sin ningún intermediario. Los intercambios se realizan con declaraciones simples, y solo se aceptan si ambas partes cumplen con las disposiciones. Fuente: Ethereum.org

d. Seguimiento de la cadena de suministros y pruebas de procedencia

En la actualidad cada parte de un producto procede de distintos lugares o compañías diferentes, se establece así toda una cadena de suministros hasta llegar a la organización que la ensambla o la elabora para comercializar el producto final, en ocasiones la cadena es tan larga que resulta difícil hacer un seguimiento completo de todo el proceso y las blockchain permiten dar seguimiento a esta cadena de suministro [96]. Una cadena de suministro se puede definir como una cadena en red de proveedores y la distribución, de cualquier producto entre el comprador final, estas se desarrollan para poder reducir costos y despegar un mercado más competitivo [100].

Figura 20: Funcionamiento de una cadena de suministro

e. Servicios de notaria

Uno de los puntos importantes es que, al dar el servicio de notaria, la economía no es un impedimento, los bloques permiten crear registros inmutables, dar

seguimiento a un documento, y verificar la autenticidad de cualquier documento, eliminando la necesidad de hacer partícipe a un tercero [96]. Aunque cabe recalcar que los servicios notariados suelen ser centralizados, pero con blockchain se puede hacer una recentralización y una reagrupación de datos por varios mecanismos [101].

Tal como lo muestra la figura 20, blockchain hacen posible dos cosas: primero certificar la prueba de que un dato existe y la propiedad de aquel, blockchain almacena la identificación de la transacción junto a una identidad única y pueden funcionar con los contratos inteligentes [102].

Figura 21: Proceso de notarización. Fuente: Safebox.

f. Servicios de seguridad automatizada

La combinación de las identidades digitales basadas en la blockchain con los contratos inteligentes, las cerraduras electrónicas del Internet de las cosas y la inteligencia artificial (IA), permitirá también crear sistemas de seguridad automatizados que garanticen o impidan el acceso a algo de personas concretas de forma completamente automática [96].

g. Voto electrónico

Aplica al anonimato de los votantes, se puede usar dentro de cualquier votación donde los participantes quieren ser desconocidos, algunas naciones consideran el blockchain como una nueva manera de plantear la democracia, tal como se muestra la Figura 21 el voto a través de blockchain permite que el conteo de votos sea de manera transparente y segura. [96].

Figura 22: Voto electrónico basado en blockchain. Se lo puede usar en votaciones generales, y específicas. Fuente CoinTelegraph

h. Creación y gestión de organizaciones autónomas distribuidas

Otra vez sale a relucir la compañía de Ethereum que idea una sociedad autónoma distribuida DAO, es una organización que se autogestiona con reglas preestablecidas y registradas en forma de código informático que se conocen como contratos inteligentes [96].

i. Gestión autónoma distribuida en ayuntamientos o gobiernos

Las DAO (figura 22) permitirían gestionar los diferentes departamentos o concejalías de un ayuntamiento, o como se conocen actualmente Gobiernos Autónomos Descentralizados; a fin de cuentas, se trata de flujos de dinero que entran y salen redistribuidos en función de las necesidades de la ciudad y sus habitantes [96]. Los servicios ofrecidos se gestionan automáticamente de forma descentralizada, son transparentes y la actividad es completamente pública [103].

Figura 23: Organizaciones Autónomas Descentralizadas. Fuente: Ethereum

BLOCKCHAIN EN ÁREAS DE GOBIERNO

El blockchain en la administración pública es cada vez mayor, alrededor del mundo más países se apegan a esta tecnología con la finalidad de tener un gobierno digital, los gobiernos podrían aprovechar el blockchain para brindar seguridad, integrar servicios de forma "hiperconectada", logrando la confianza y responsabilidad; no solamente podrían incluir monedas digitales, también se pueden realizar pagos, registro de tierras, identidades digitales, trazabilidad en cadenas de abastecimiento, salud, registro de transacciones, votaciones y gestión de entes legales [104].

A continuación, se lista algunos países que están apegándose al uso de las tecnologías blockchain, entre los años 2017-2020.

- **NORTEAMÉRICA**
  - **Canadá**
    - El Programa de Asistencia a la Investigación Industrial de la NRC (NRC IRAP), organizó una sesión de inicio de blockchain y dio a conocer sus planes para probar la viabilidad de la tecnología blockchain en la administración de los acuerdos de contribución del programa (financiación de la innovación). El experimento proporcionaría un primer caso de uso real de este tipo para el gobierno y otras instituciones públicas. [105].
    - El Gobierno de Canadá (GC) está utilizando la tecnología blockchain para emitir a los empleados basados en proyectos una especie de CV digital, proporcionando "un registro permanente, propio y seguro de sus habilidades y experiencias" [106].
  - **México**
    - El expresidente Vicente Fox trabaja en un proyecto que integra blockchain con actividades agrícolas. Fox se encontraba en plena investigación de blockchain para aumentar la transparencia y reducir la corrupción dentro del gobierno mexicano [107].
  - **Estados Unidos**
    - La Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) está comenzando a experimentar con blockchain para crear una plataforma más eficiente y segura utilizando un protocolo blockchain que permitirá al personal desde cualquier lugar transmitir mensajes a través de numerosos canales de un libro mayor descentralizado. La aplicación se utilizará de diferentes maneras, incluida la facilitación de la comunicación entre las unidades y la sede, y transmitir información entre los oficiales de inteligencia y el Pentágono [108].

Figura 24: Casos de estudio, en Norteamérica.

- **CENTROAMERICA**
  - **El Salvador**
    - En El Salvador la iniciativa del presidente Nayib Bukele, se convirtió en septiembre en el primer país en establecer el bitcoin como moneda legal en curso, a la par del dólar estadounidense, en octubre Bukele anunció que convirtió unos 25 millones de dólares de las reservas nacionales a bitcoins; el gobierno ha presentado la medida como una forma de impulsar el desarrollo económico [109].

Figura 25: Caso de estudio en Centroamérica

- **SUDAMERICA**
  - **Ecuador**
    - En Ecuador existió un proyecto que intento vincular a la sociedad con el dinero digital en 2014. El gobierno gasta más de $ 3 millones cada año para cambiar billetes viejos deteriorados por dólares nuevos. En

febrero de 2015, la DE actuaba como un medio de pago práctico. Sin embargo, el 71% de las cuentas abiertas permanecieron inactivas ya que los ciudadanos se mostraron reacios a aceptar una nueva moneda y, en general, desconfiaron del Gobierno [110].

- **Argentina**
  - Un proyecto de identidad digital para la inclusión basado en blockchain ha sido anunciada en Argentina, con el objetivo de mejorar el acceso de los ciudadanos a los servicios gubernamentales [111].

Figura 26: Casos de estudio en Sudamérica.

- **EUROPA**
  - **Austria**
    - El gobierno austriaco debutó el nuevo Instituto de Investigación para la Cripto-economía, que apoyará proyectos de investigación de blockchain a través de un fondo de € 8 millones [112].
  - **Estonia**
    - El gobierno de Estonia ha estado probando la tecnología desde 2008 y fue el primer país en usar blockchain a nivel nacional [113].
    - El Ministerio de Justicia de Estonia aprovechó la tecnología blockchain para crear el sistema e-Law, una base de datos en línea que permite al público leer todos los proyectos de ley presentados desde febrero de 2003 [113].

- **España**
  - El Ayuntamiento de Valls estrena el proyecto del Portal de Datos Municipal, que publica conjuntos de datos y recursos en el portal web municipal local y en la cadena de bloques, a través de IPFS [114].

Figura 27: Casos de estudio en Europa

- **ÁFRICA**
  - **Ghana**
    - Bitland, basada en blockchain, busca abordar el problema de las tierras no registradas en África occidental. El gobierno de Ghana, en asociación con Bitland, lanzó un proyecto piloto para registrar tierras en una cadena de bloques. Más del 78% de la tierra de Ghana no está registrada. El proyecto ya se ha probado en 20 comunidades de Kumasi [115].
  - **Sudáfrica**
    - La Alianza Nacional de Blockchain de Sudáfrica (SANBA) se formó para Establecer una asociación entre el gobierno, las empresas, la academia y la sociedad civil para apoyar el uso de tecnologías blockchain. en el contexto sudafricano [116].
  - **Tanzania**
    - Tanzania dice que más de 10,000 'trabajadores fantasmas' fueron eliminados de la nómina del gobierno utilizando la tecnología blockchain para auditar la nómina pública [117].

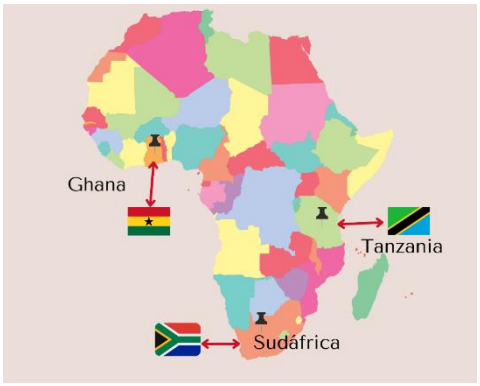


Figura 28: Casos de estudio África

- **ASIA**
  - **China**
    - El Comité de Gestión del Nuevo Distrito de Xiong'an anunció oficialmente la introducción de la tecnología blockchain en la gestión gubernamental, también para crear una ciudad inteligente; para establecer un gobierno limpio, transparente y eficiente a través de una supervisión integral [118].
  - **Corea del Sur**
    - El gobierno coreano liderará 6 pilotos de blockchain con un fondo de $ 9 millones. El objetivo principal, según el documento, es mejorar la eficiencia y transparencia del intercambio de información en estos servicios públicos mediante el uso de una red distribuida [119].

Figura 29: Casos de estudio en Asia

2.3. MARCO TEÓRICO

2.3.1. BLOCKCHAIN EN LA ADMINISTRACIÓN PÚBLICA

La implementación de blockchain en la administración pública surge por la falta de confianza en las transacciones qué se realizan de manera económica, jurídica o burocrática. En la publicación "Blockchain en la Administración Pública", los autores Florencia Serale, Christoph Redl y Arturo Muente-Kunigami, dejan claro qué para aplicar blockchain se deben tomar en cuenta una serie de eventos como: formalizar la creación de un espacio para la experimentación, diseñar para escalar, tener un enfoque holístico tanto en la aplicación como en su evaluación y finalmente capacitar al personal que estará a cargo de la aplicación, todo esto debe cumplirse para crear blockchain dependiendo del caso de uso que se le quiera dar, otro aspecto a tomar en cuenta es conocer si la institución está en la posibilidad de asumir los costos qué implica tener un blockchain [120].

Además de conocer de antemano para qué sirve, como funciona y si es necesario aplicarlo; existen variedad de enfoques de blockchain desde la creación de una identidad digital a través de prueba criptográfica, asegurar la integridad de los datos hasta incrementar la transparencia de los procesos. Para poder llevar a cabo la cadena de bloques es necesario estudiar el área, realizar el test para conocer a qué tipo de blockchain se apega en la institución y así escoger la que realmente ayudará [120].

2.3.2. ESTUDIO EXPLORATORIO SOBRE LA TECNOLOGÍA BLOCKCHAIN APLICADA EN CADENA DE SUMINISTRO

El estudio exploratorio de parte de Marisol Barrón, Elizabeth de la Torre, Bernardo Hernández sugiere como el blockchain puede usarse en la cadena de suministro, asimismo explica cómo puede usarse dentro del sector financiero, el sector de la salud, para el bienestar social, la industria alimentaria, el sector automotriz y el sector aeronáutico, también hace referencia a casos de éxito como por ejemplo la facilitación en el comercio internacional, o la cadena de suministro ética [121].

Como el trabajo anterior, también menciona algunos de los elementos tecnológicos para aplicar tecnologías blockchain, habla acerca de los tipos de redes, la fiabilidad de la tecnología, quiénes son los participantes, qué plataformas informáticas se puede usar en blockchain y blockchain como servicio; además explica alguna de las características de blockchain que permiten que sea una tecnología que pueda usarse y que tenga éxito. Una parte fundamental de las tecnologías blockchain es la seguridad que brinda, por ejemplo, utiliza pruebas criptográficas, claves hash, entre otros aspectos de seguridad [121].

2.3.3. BLOCKCHAIN EN EL SECTOR PÚBLICO, UNA PERSPECTIVA INTERNACIONAL

El mundo está cambiando rápidamente y gran parte de este cambio se debe a la presencia de las tecnologías de información que han tenido una influencia radical en cómo nos comunicamos y cómo se gestionan los procesos. En el artículo titulado "Blockchain el sector público, una perspectiva internacional" se toma en cuenta la tecnología de cadenas de bloques de naturaleza disruptiva e innovadora, siempre y cuando la seguridad, la interoperabilidad, la eficiencia y la automatización sean los principales requisitos para poder crear una cadena de suministro que permita ofrecer nuevas oportunidades en el sector público [122].

El blockchain en el sector público permitiría mejorar la transparencia y mantener la confianza de parte de la ciudadanía, este artículo relata también cómo la Unión Europea toma iniciativas respecto al tema también hace hincapié en el uso de la Administración pública y la transformación digital haciendo uso del gobierno abierto y menciona varios casos de uso como, por ejemplo: el voto electrónico, los certificados y diplomas en el campo de la enseñanza, el seguimiento y regulación de mercados. Asimismo, habla acerca del proyecto piloto del TCE qué se enfoca en estimular el progreso de la tecnología de cadenas de bloques en el ámbito de la auditoría en la Unión Europea y explorar la aplicación en práctica [122].

Otro ejemplo mencionado dentro del artículo publicado por Magdalena Cordero Valdavida es el proyecto ECA que registra la huella digital de cada documento o información registrada conteniendo esta huella y registrándola en la cadena de bloque pública. Algunos beneficios mencionados son: evitar el problema de incumplimiento de la ley de protección de datos, qué la información registrada sea pequeña y que el sistema se ocupa del registro en el blockchain público con lo que el usuario no percibe problema de lentitud del sistema [122].

CAPÍTULO III

3. DESARROLLO DE LA PROPUESTA

3.1. REQUERIMIENTOS

Según la guía de referencia para la adopción de blockchain existen claves que se deben tomar en cuenta ante la implementación de cualquier proyecto basado en cadenas de bloque.

REQUERIMIENTOS	
R01	Levantamiento de información a través de estudio bibliográfico, y a realización de entrevista y cuestionario al personal encargado del Departamento de Sistemas y Comunicaciones de la Municipalidad en estudio.
R02	Uso de la metodología ADDIE para poder completar el desarrollo de la simulación de las cadenas de bloque.
R03	Realización de un estudio profundo a través de la investigación acerca de las Bases de Datos relacionales y no relacionales; junto con la tecnología de Blockchain; en temas relacionados a características, funcionamientos, ventajas, desventajas, seguridad informática.
R04	Cuadro comparativo de BD relacionales y no relacionales como MySQL, Postgre SQL, SQL Server, Mongo DB, Redis, Apache Cassandra. Y en función de las bases de datos, realizar una comparativa con el Blockchain
R05	A través del análisis del cuestionario, escoger herramientas necesarias para el Blockchain, y también el modelado de BD
R06	Demostrar que tipo de blockchain cumple con los requisitos necesarios y que permitan una adaptación sencilla a la municipalidad.
R07	Analizar la ley ecuatoriana para aplicar y vincular al proyecto desarrollado.
R08	Instalación de máquinas virtuales Anaconda (Python), Visual Studio Code, Spyder. Instalación de extensiones Metamask, Remix IDE
R09	Instalación de herramienta Xampp
R10	Requisitos mínimos por tomar en cuenta para el desarrollo del proyecto, es tener a disposición una máquina que mantenga **SO:** Windows 10/11; **Procesador:** Intel Core i3/ AMD Ryzen 5 3450U; **Memoria:** 4 GB de RAM: **Almacenamiento:** 6 GB de RAM.
R11	Una conexión estable a internet para realizar la simulación de Blockchain, debido al rendimiento de cada transacción en las cadenas de bloque, se conoce

	que pueden llegar entre 15 a 40 por segundo. Además de depender de la latencia, el tamaño de la red, el tamaño de transacciones y el proceso de consenso usado.
R12	Aplicación de criptografía a través de SHA256
R13	Demostrar en la simulación a través de una interfaz que el sistema que contenga Blockchain es intuitivo al usuario
R14	Analizar Blockchain y la cadena distribuida
R15	La capacidad operacional del sistema, al momento del tiempo de durabilidad de cada transacción.
R16	Presentar la documentación sobre los beneficios y las ventajas de adaptarse a las tecnologías blockchain

Tabla 4: Requerimientos para el cumplimiento del proyecto

3.2. ANÁLISIS COMPARATIVO DE BASES DE DATOS

Para poder agilizar el estudio de las técnicas tradicionales de almacenamiento es importante reconocer sus diferencias entre las bases de datos relacionales y no relacionales, ya que al ser enfocadas al análisis de diferentes volúmenes de datos hacen que sean desiguales entre sí, pero tiene el mismo objetivo almacenar información. Este análisis se realiza con la ayuda de la información obtenida en el capítulo II, dentro del levantamiento de información y se presenta en la Tabla 5.

BASES DE DATOS		
	RELACIONALES	NO RELACIONALES
Estructura	Estructura de tablas y columnas. Se denominan SQL.	Estas se basan en documentos, no tienen relaciones. Son denominadas NoSQL.
Lenguaje de consulta	Usan lenguaje SQL o lenguaje estructurado	El lenguaje usado NoSQL usa lenguajes de consultas no declarativos.
Capacidad	Las BD relacionales no pueden usarse en instituciones que necesite almacenar información jerárquicamente.	Al admitir el método clave-valor, hace posible que puedan servir de almacenamiento jerárquico.
Escalabilidad	Son escalables ya que pueden aumentar sus filas, por lo que se puede expandir.	Las NoSQL, son escalables horizontalmente, ya que usan formatos de documentos.

Transacciones	Trabajan con ACID "atomicidad, consistencia, aislamiento y durabilidad."	Usa el teorema de CAP "consistencia, disponibilidad y tolerancia al particionado"

Tabla 5: Tabla Comparativa BD relacional y no relacional

Existen un sinnúmero de características que pueden ser útiles para hacer comparaciones entre las bases de datos. En la siguiente Tabla 6, se podrá visualizar aspectos claves como los desarrolladores, seguridad, transacciones de las bases de datos relacionales como MySQL, Postgre SQL, SQL Server; y las no relacionales en la Tabla 7 : Mongo DB, Redis, Apache Cassandra.

COMPARATIVA BASES DE DATOS RELACIONALES			
Nombre BD / **Característica**	**MySQL**	**Postgre SQL**	**SQL Server**
Servicios en la nube	Si	Si	Si
Desarrolladores	Oracle Corporation	Enterprise DB	Microsoft
SO	Multiplataforma	Multiplataforma	Linux, Windows
Lenguaje query	SQL	SQL	SQL
Transacciones	Complejas	Simples-complejas	Complejas
Integridad	ACID	ACID	ACID
Modo de replicación	Maestro - Maestro/esclavo	Maestro-esclavo	Transaccional, Merge, Snapshot, Peer-to-peer, Bidireccional
Disponibilidad	Alta	Alta	Alta
Licencia	Licencia dual: Licencia pública general/ Licencia comercial por Oracle Corporation	Licencia Open Source	Licencia comercial. Edición empresarial $13.748

Tabla 6: Comparativa BD Relacionales

COMPARATIVA BASES DE DATOS RELACIONALES			
Nombre BD / **Característica**	**Mongo DB**	**REDIS**	**Cassandra**
Servicios en la nube	Si	Complicada	Si
Desarrolladores	Mongo DB Inc.	Salvatore Sanfilipo/ AWS	Apache Software Foundation

SO	Windows, GNU/Linux, OS X y Solaris	Linux y OS X	Unix o Linux, MAC OSX, Windows
Lenguaje query	Javascript	C, C++, Java, Python, PHP, entre otros.	Cassandra Query Language CQL
Transacciones	Simples	Simples	Complejas
Integridad	BASE	Memoria de código abierto	ACID
Modo de replicación	Primario-secundario	Maestro-esclavo	Peer-to-peer
Disponibilidad	Alta disponibilidad en conjunto de replicas.	Alta	Alta
Licencia	Licencia AGPL	Licencia BSD	Licencia de Software Apache v2.0

Tabla 7: Comparativa de BD No Relacionales

3.3. BASE DE DATOS

Al ser un proyecto investigativo, la estructura realizada es a partir de información adicional expresada libremente por miembros de la municipalidad y también a la investigación acerca de temas relacionados a servicios ofrecidos por los GAD´s.

Por lo cual los puntos clave en el servicio de Catastros y Avalúos en relación con el pago de podrían ser:

- Información relacionada con el ciudadano como: Nombres completos, cedula, dirección, número telefónico, numero celular, estado civil, si cuenta con servicios bancarios, etc.
- Información relacionada con la descripción de los bienes que posee una persona
- Solicitudes para informes técnicos
- Solicitudes para visita preliminar y localización
- Información de georreferencia
- Información de Impuestos prediales
- Información referente a la ubicación del bien

3.4. ANÁLISIS COMPARATIVO BLOCKCHAIN

Sin duda las bases de datos son muy útiles en entidades gubernamentales; ya que la capacidad y la cantidad de datos procesados son sumamente grandes; atienden a toda una

población especifica, además de atender locales comerciales, y todo lo que tiene que ver con servicios de información, cobros, coactivas, predios urbanos, terrenos, etc.

Sin embargo, al tener un centro de datos dentro del mismo edificio y de la misma área, no disponer de servicios en la nube, hacen que la integridad, confidencialidad, disponibilidad de los datos sean sensibles ante ataques cibernéticos; también el hecho de que los protocolos de seguridad no son los acordes, debido a que la entrada al centro de datos no posee las medidas de seguridad necesarias, el personal de la municipalidad pueden ingresar al área de Sistemas, estas acciones vuelven vulnerable a la información "resguardada" del edificio. Otro de los aspectos a tomar en cuenta al usar bases de datos, es el hecho que se contrata servicios por intermediarios dependiendo de ellos para asegurar la información.

Ante estos "problemas", hace algún par de años las tecnologías blockchain se han vuelto una elección para manejar los datos de las administraciones gubernamentales, permitiendo que la información sea segura, sin intermediarios, y que no se pueda modificar sin las credenciales necesarias.

Esto conlleva al análisis de las características generales de una base de datos vs blockchain en la Tabla 8; los puntos en cuestión son la autoridad, arquitectura, manejo de datos, integridad, transparencia y rendimiento.

CARACTERÍSTICAS	BASE DE DATOS	BLOCKCHAIN
Autoridad	Administrador Centralizada	No necesita administrador al menos que sea una Blockchain centralizada Descentralizada
Arquitectura	Cliente – servidor	Registro distribuido
Manejo de datos	CRUD (crear, leer, actualizar y borrar)	Opción de lectura y escritura
Integridad	Depende de la entidad	Datos íntegros, precisos y coherentes
Transparencia	El administrador decide los roles	Depende si es Blockchain publica o privado
Rendimiento	Trabaja con servidores, los procesos sueles ser rápidos	Depende del uso, de las verificaciones de proceso y del consenso utilizado.

Tabla 8: Comparativa de BD y Blockchain

Al estudiar más acerca de las cadenas de bloque es necesario hacer una elección de que tipo de blockchain es necesaria para la municipalidad, por lo que gracias a la investigación se presentan las características de cada una de ellas, en la Tabla 9.

	PÚBLICA	PRIVADA	HÍBRIDA
Tiene varios participantes.	Si	No	No
Los usuarios actúan como nodos	Si	No	No
Transparencia	Si	A veces	A veces
Único administrador	No	Si	No
Existe más de un administrador	No	No	Si
No hay administradores	Si	No	No
Igualdad de roles entre los usuarios	Si	No	No
Implementación de Smart contracts	Si	Si	Si
Recompensa por minado de bloques	A veces	No	A veces
Confiabilidad	Si	No	A veces
Seguridad basada en el protocolo de consenso	Si	No	A veces
Seguridad basada en hash	si	A veces	A veces

Tabla 9: Tipos de blockchain

Gracias a la investigación previa y al análisis del cuestionario realizado al personal del departamento de Recursos Tecnológicos y Sistemas que se encuentra en la parte de "Metodología de la Investigación", se puede determinar qué tipo de blockchain es necesaria para la Municipalidad en este caso se trata de una **Blockchain Hibrida /orientada más a una BC privada**. Ya que al ser una entidad gubernamental no todos los datos pueden ser públicos, y no todos pueden administrarlos.

3.5. FUNCIONAMIENTO CADENA DE BLOQUES

Las cadenas de bloques son conocidas por agrupar los datos en bloques y cada uno de ellos se enlaza el uno con el otro como si fuera una cadena. Una vez que se registra la información dentro del bloque es difícil modificarlo o cambiarlo, cada bloque tiene los siguientes datos: el valor del Hash del bloque y el valor del Hash del bloque anterior, la

información guardada o almacenada dentro de cada bloque, timestamp, nonce la información agrupada en cada bloque tiene que estar validado por el sistema; para ello se usa una huella digital o clave criptográfica está clave es denominada “Hash” la cual es única y no se puede modificar [27].

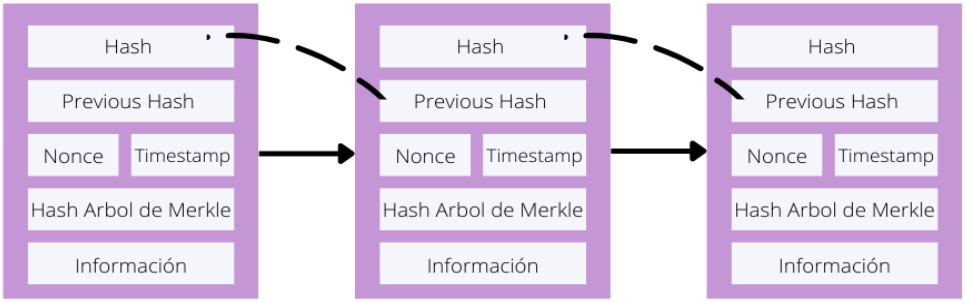


Figura 30: Estructura de un Bloque en Blockchain. Elaboración propia

Tal como se muestra en la Figura 30, un bloque se encuentra estructurado de manera que todos queden comunicados entre si a través de la creación de un hash previo, a cada cadena se la puede conocer como transacción. Cada transacción es casi imposible de modificar o alterar, pero si es posible verla. Recordar que Blockchain es una base de datos distribuida, pero para que cada transacción sea ejecutada, debemos tener en cuenta que se realizan a través de dos partes; por ejemplo, en el caso de bitcoin: “Maria envia 50 dolares a Mario”. Esta información es enviada a todos los nodos que conforman la red de Blockchain. Por lo que todos tienen una copia exacta de los datos existentes en la cadena, por lo que falsear la información es casi imposible, si alguien la modifica tendría que alterar toda la cadena.

En el capítulo dos se explicó algunos de los beneficios que tienen las cadenas de bloque, así que cada transacción se caracteriza por ser inmutable, transparente, integra, entre otras. Otro de los aspectos a tomar en cuenta dentro del bloque es la función hash que usan, por lo general esta función aplica un algoritmo sobre alguna entrada de datos, generando así una respuesta de tamaño predeterminado; los hashes son funciones que usan una sola dirección, si se coloca la misma entrada siempre da el mismo resultado, pero si algo se modifica dentro de la información, el valor cambia, así es más fácil ver si el contenido ha sido cambiado [123]. Dependiendo de la Blockchain a implementar y según las herramientas a usar, el sha256 suele modificarse, por ejemplo, Ethereum suele usar valores uint para hashear la información, específicamente KECCAK-256. Un punto interesante que tomar en cuenta es que la información de entrada puede ser de valores largos o cortos, el tamaño del hash no varía

Figura 31: Función sha256 con datos.

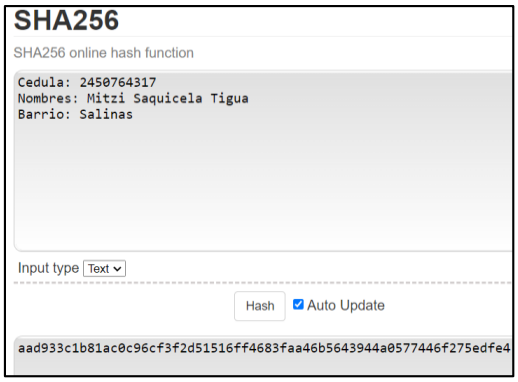


Figura 32: Cambio de datos, por lo que se altera el sha 256

3.6. EL BLOQUE

Dentro del capítulo dos de este proyecto, se menciona características generales de lo que es Blockchain, sin embargo, en este punto se especificara información acerca del bloque en sí. El bloque es el punto inicial para crear una blockchain, como se explicó anteriormente si un bloque es modificado los valores de hash no serán los mismos, por lo que el bloque será invalido y la cadena mostrará este error. Como se mostró en la figura 30, los bloques poseen un hash propio, un previo hash, un nonce, un timestamp.

El nonce es un número aleatorio que no es posible predecir, se relaciona con el hash asociado con la información que contiene el bloque, este sirve para evitar manipulación de este; la función del hash con el nonce se conoce como minación del bloque; además de funcionar como prueba de trabajo y el algoritmo de consenso [123].

El timestamp es una marca temporal que nos enseña la fecha, la hora en la que se ha creado el bloque

Transaction o date, son las operaciones realizadas en la blockchain, además puede representar un token enviado o recibido entre un usuario u otro, tienden a funcionar en los Smart contracts.

IMPLEMENTACIÓN DE BLOCKCHAIN

Existen varias herramientas de código abierto que pueden ayudar a la creación de blockchain entre ellas podemos mencionar: Ethereum, Hyperledger, Corda, Alastria, Ripple, Stella, Qurom.. estas trabajan como redes públicas o privadas. Para este trabajo se escogió Ethereum ya que nos permite crear Smart contracts en lenguaje solidity y compilarlos de manera sencilla, sin el uso de más aplicaciones que usarían más recursos de la computadora. En un ambiente público, para el uso de Ethereum, se debe conectar a

una cartera que nos permite almacenar la transacción, en este caso hicimos uso de Metamask de la cuenta de Rinbekey, además de revisar las transacciones en tiempo real en Etherscan. Otra de las herramientas a usar es visual studio code, en unión con extensiones de pug, node js, i18n, entre otras; para demostrar cómo trabaja una cadena.

CRIPTOGRAFÌA

Para conocer más acerca del funcionamiento de la cadena de bloques, es necesario reconocer como trabajan criptográficamente, esta función permite que el blockchain sea inmutable e integro.

- **Función hash:**

Es una operación criptográfica que genera un valor único e irrepetible, a partir de la información dada. En el caso de blockchain, se usa SHA25,6, es un hash de 256 bits. El identificador no puede ser revertido o cambiado, por lo que es conocido como un método ideal para las cadenas de bloque, la resistencia a las colisiones es casi nulas, ya que un hash es diferente al otro.

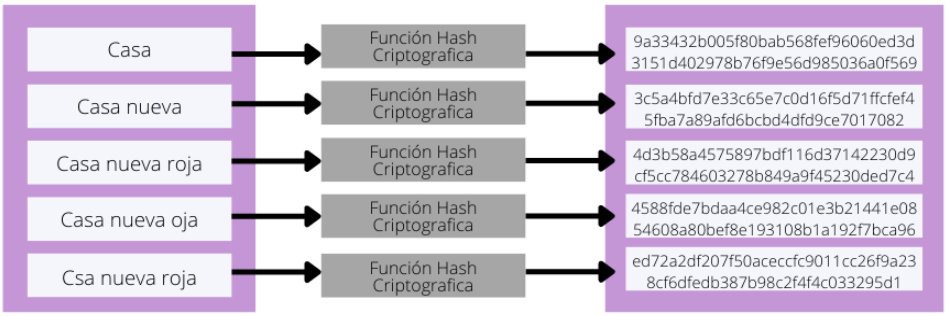


Figura 33: Esquema sobre el funcionamiento de hash

Cada entrada tiene una representación criptográfica diferente, las propiedades de una función hash permiten que los bloques sean seguros y confiables [123], estas características son:

Computación eficiente: el equipo de cómputo debe ser capaz de realizar la labor matemática en la que se cera un valor hash, este debe ser en un tiempo corto.

Determinista: esto implica que el mismo mensaje (entrada) debe producir siempre el mismo digest (salida), cada vez que sea consultado

Resistente a preimagen: la salida no debe revelar ningún dato de la entrada. El hash debería tener siempre la misma longitud en la salida, independientemente del tamaño del mensaje.

Resistente a colisión: jamás se puede producir dos mensajes de salida iguales, es decir el hash.

- **Infraestructura de clave pública y firma digital**

Cada bloque posee una clave publica, la cual se comparte en el resto de los nodos de la red, este valor identifica al mismo y también tiene una clave privada a la que solo el usuario tiene acceso; esta forma permite que se pueda firmar cada transacción y asimismo verificar que se han realizado por el usuario, ya que ambas llaves se encuentran relacionadas matemáticamente.

Todos los algoritmos deben tener las siguientes características : autenticación: esta debe ser capaz de asegurar al destinatario que la transacción proviene de un remitente especifico, los datos de la firma son precisos por lo que son casi imposibles de falsificar; integridad: esta propiedad estima que los datos llegaran de manera intacta al remitente, no pueden ser modificados de ninguna forma durante la transferencia, si algún atacante logra modificarla la firma varia por lo que la transacción es invalida; no repudio: el usuario que firma digitalmente no puede negar lo que realizo, esto se refiere a un concepto legal [124].

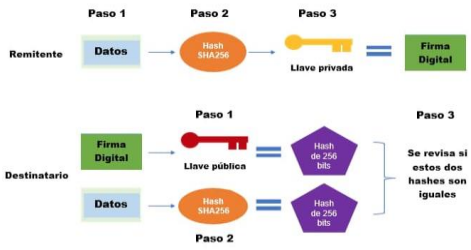


Figura 34: Funcionamiento de una firma digital + una función criptográfica. Fuente: Criptonoticias.

3.7. COMENZANDO LA CADENA DE BLOQUES

Primero se debe conocer para servirá y a quien prestará los servicios las cadenas de bloque, este trabajo investigativo pretende demostrar como el Blockchain puede ayudar a la ciudadanía y a la municipalidad para evitar el robo de información o ataques relacionados que rompan la integridad de los datos. en la siguiente imagen se podrá observar en medida base de como los servicios de blockchain serian, no es diferente al proceso de acercarse a una ventanilla a pedir información.

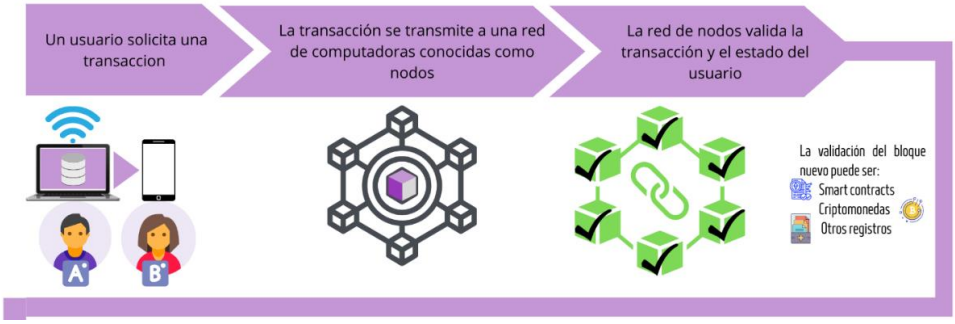


Figura 35:Proceso simple de blockchain. Fuente: Elaboración propia

Figura 36:Proceso simple de blockchain. Fuente: Elaboración propia

El entorno virtual para poder establecer la cadena de bloques es en conjunto de una serie de programas que permiten así poder crear el blockchain. En este caso se usa un entorno virtual anaconda, la herramienta de visual studio code.

Python es un lenguaje muy sencillo y fácil de aprender. Además de permitir al programador entender su código. El código puesto en escena es acerca de la creación una cadena de bloques, empezando desde el bloque génesis, la minación del bloque y comprobar si la cadena es válida, el Anexo 4 muestra la imagen de la herramienta usada.

CÓDIGO USADO PARA CREACIÓN DE UNA CADENA DE BLOQUES

```
# CREANDO UN BLOCKCHAIN
import datetime
import hashlib
import json
from flask import Flask, jsonify

# Paso 1 - Armando el Blockchain

class Blockchain:
    #bloque genesis    #define funcion init y para realizar el minado
    def __init__(self):
        self.chain = []
        self.create_block(proof = 1, previous_hash = '0')

    def create_block(self, proof, previous_hash):
        block = {'index': len(self.chain) + 1,
                 'timestamp': str(datetime.datetime.now()),
                 'proof': proof,
                 'previous_hash': previous_hash}
        self.chain.append(block)
        return block

    def get_previous_block(self):
        return self.chain[-1]

    def proof_of_work(self, previous_proof):
        new_proof = 1
        check_proof = False
```

```
        while check_proof is False:
            hash_operation = hashlib.sha256(str(new_proof**4 -
previous_proof**2).encode()).hexdigest()
            if hash_operation[:6] == '000000':
                check_proof = True
            else:
                new_proof += 1
        return new_proof

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

    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**4 -
previous_proof**2).encode()).hexdigest()
            if hash_operation[:6] != '000000':
                return False
            previous_block = block
            block_index += 1
        return True

# Paso 2 - Minando el Blockchain

app = Flask(__name__)
blockchain = Blockchain()

# Minando un Nuevo Bloque
@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,minaste un bloque!',
                'index':block['index'],
                'timestamp':block['timestamp'],
                'proof':block['proof'],
                'previous_hash':block['previous_hash']}
    return jsonify(response), 200

# Obteniendo Cadena Completa
@app.route('/get_chain', methods=['GET'])
```

```
def get_chain():
    response = {'chain':blockchain.chain,
                'length':len(blockchain.chain)}
    return jsonify(response), 200

# Chequeando validez de cadena de bloques
@app.route('/is_valid', methods=['GET'])
def is_valid():
    is_valid = blockchain.is_chain_valid(blockchain.chain)
    if is_valid:
        response = {'message':'Valido'}
    else:
        response = {'message':'No es valido!'}
    return jsonify(response), 200

# Corriendo el App

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

Una vez escrito el código que se usara para la creación y minación de bloque se procede a comprobar si se puede realmente usar en la web. Para esto se usa el programa de Postman, así es más fácil lanzar el programa.

La herramienta de Postman permite manejar el código sin interfaz, se presenta a través de la Tabla 10, cómo funciona la cadena de bloques con el código escrito en Spyder de Anaconda con lenguaje Pyhton.

Creación de bloque Genesis, para esto se hace uso del get


```
{
    "chain": [
        {
            "index": 1,
            "previous_hash": "0",
            "proof": 1,
            "timestap": "2021-09-01 23:17:07.869652"
        }
    ],
    "length": 1
}
```


Figura 37: Creación de bloque Genesis

Luego la dirección: http://127.0.0.1:5000/mine_block
Minación del bloque, se pasa del bloque genesis el hash, y esta clave única es traspasada al nuevo bloque.


```
{
    "index": 2,
    "message": "Felicidades, minaste el bloque!",
    "previous_hash": "487a7324064269a6c98e336b37f64ec9a0a13cb377f614ba99a1b5aad986a689",
    "proof": 2,
    "timestamp": "2021-09-01 23:48:50.366378"
}
```


Figura 38: Concadenar la cadena

Finalmente, se escribe http://127.0.0.1:5000/get_chain

Para crear un nuevo bloque que ya contendrá el hash previo del bloque anterior, y la prueba de trabajo que uso, a la vez también comparte el tiempo de creación de bloque.

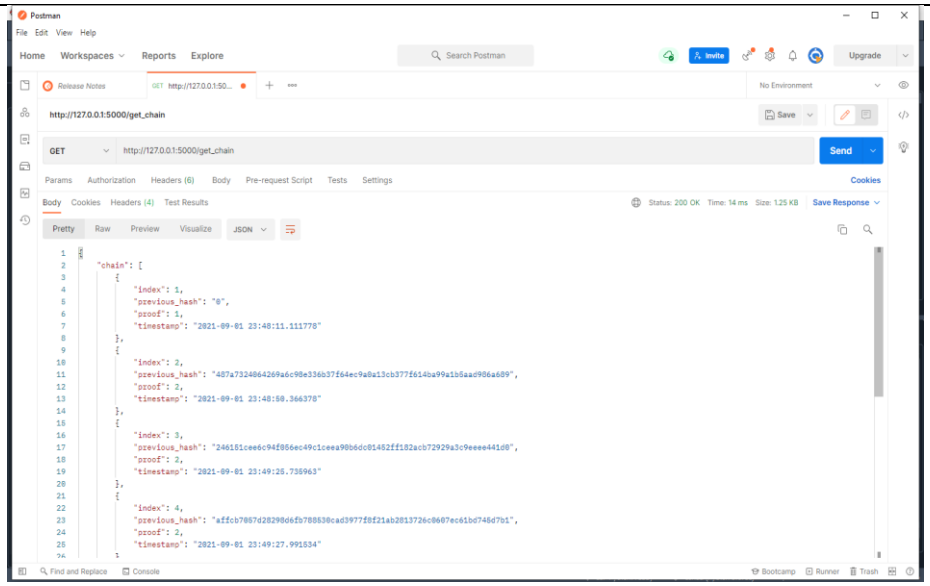


Figura 39: Blockchain con varios bloques

Tabla 10: Uso de Postman + spyder de Anaconda

ESCENARIO 1 – FUNCIONAMIENTO BÁSICO DEL BLOCKCHAIN

Esta es una muestra de cómo funcionan las cadenas de bloque en medida de ingresar información, obtener un hash, un previous hash. Este serviría para ingresar información que mantenga un usuario determinado, un registro único que en este caso sería el nonce, un hash y previous hash; este sería una base para el servicio de Catastros y Avalúos: el ingreso de usuarios respectivamente, que mantiene información del ciudadano, además de información previa al lugar de vivienda.

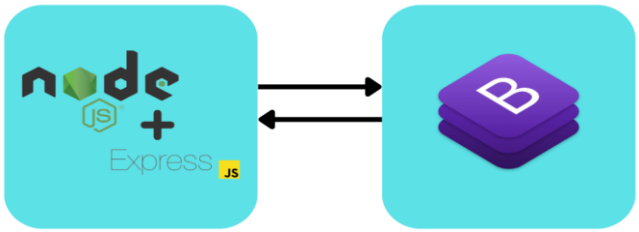


Figura 40: Arquitectura del escenario 1

Se hizo uso de node js, y para la interfaz gráfica Bootstrap un conjunto de herramientas para el diseño de sitios web. Esta parte seria administrativa ya que el ingreso de la información seria por parte de la municipalidad. Una cadena de bloques con una base de datos distribuida, junto con un servidor externo, se podría diagramar de la siguiente manera

En el siguiente grafico encontrara un diagrama que explica en breve como funcionaria una red blockchain dentro de un municipio, al momento de registrar un usuario o varios al mismo tiempo, se observa la creación del bloque génesis, y su hash único , existen varios usuarios

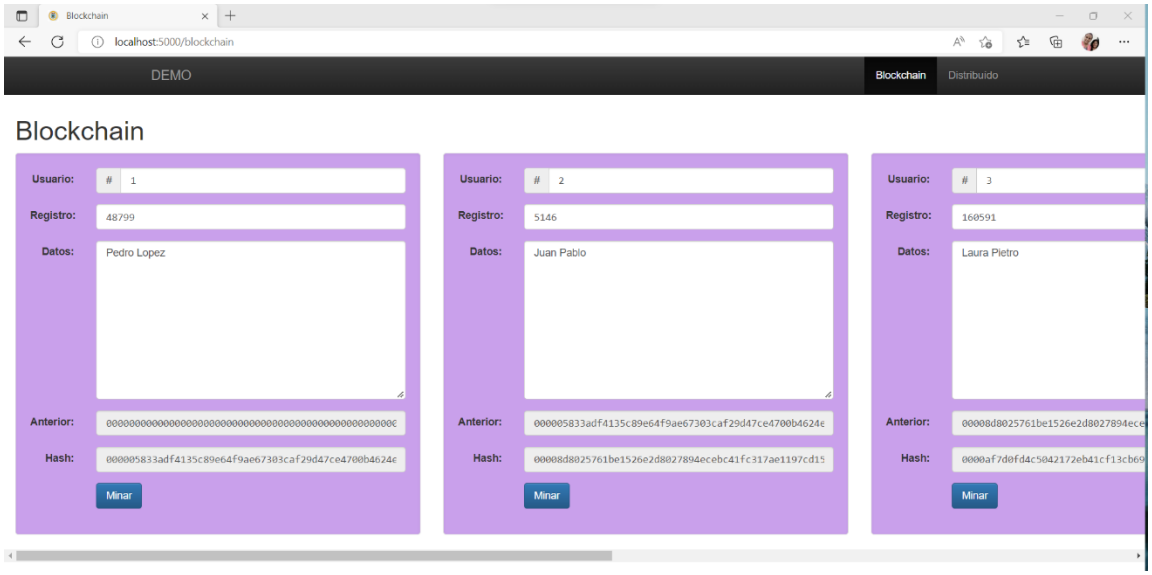


Figura 41: Dentro de localhost:5000. Se encuentra la información registrada de manera correcta por lo que se procede a minar. La minación permite crear los hashes necesarios. El propio del bloque y el que pasara al siguiente bloque.

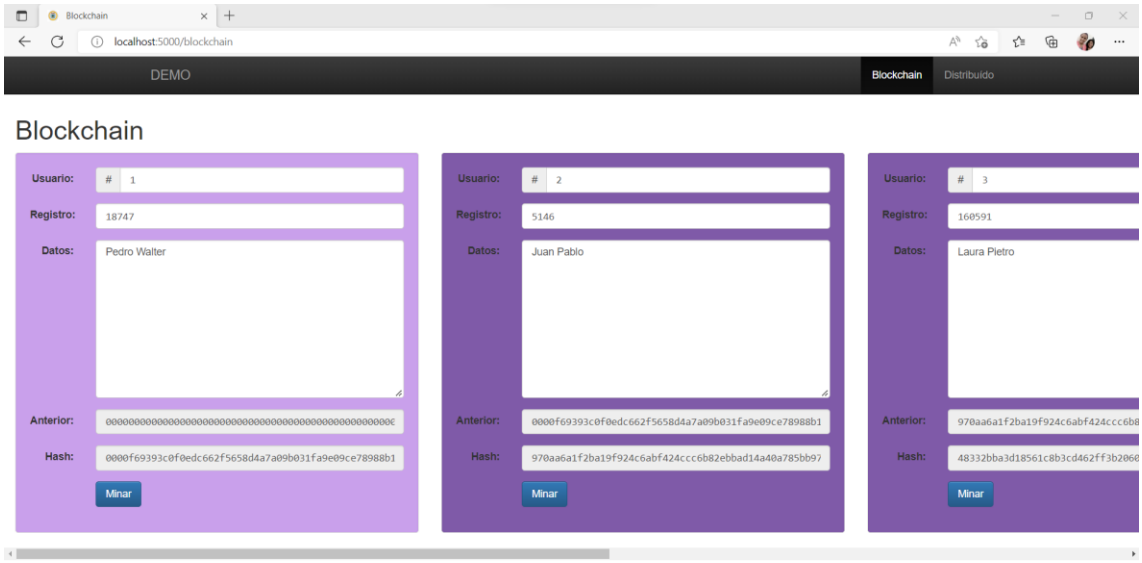


Figura 42: Si no se selecciona la palabra Minar, los bloques no son capaces de crearse, por lo tanto, la cadena solo tiene un bloque Genesis. El cual tiene un nonce y un hash con proof of work que permite que aparezcan 4 ceros antes del hash

En este punto se presenta una cadena distribuida que tienen como título CADENA A y CADENA B, con dos cadenas de bloque que contienen 5 bloques, cada una de ellas.

Estas demuestran que la información registrada por igual obtendrá como resultado el mismo hash, aunque se encuentren en cadenas de bloque diferente, pero la cadena distribuida actúa de diferente manera.

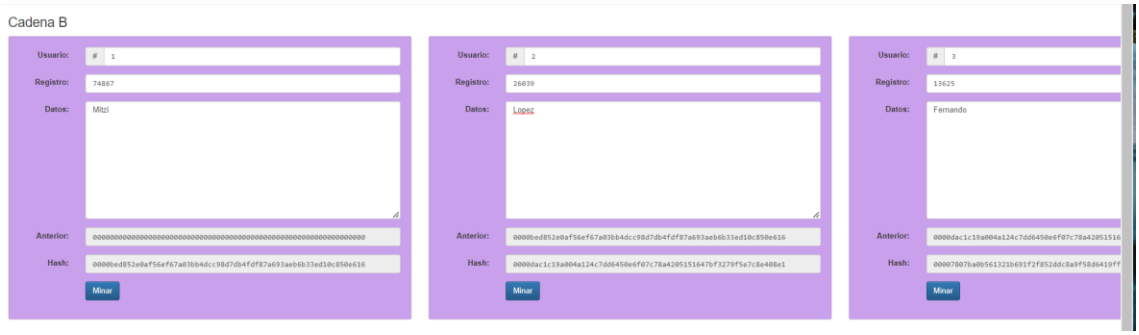


Figura 43: La cadena A, tiene información minada en su bloque génesis el cual tiene como hash "0000f69393...."

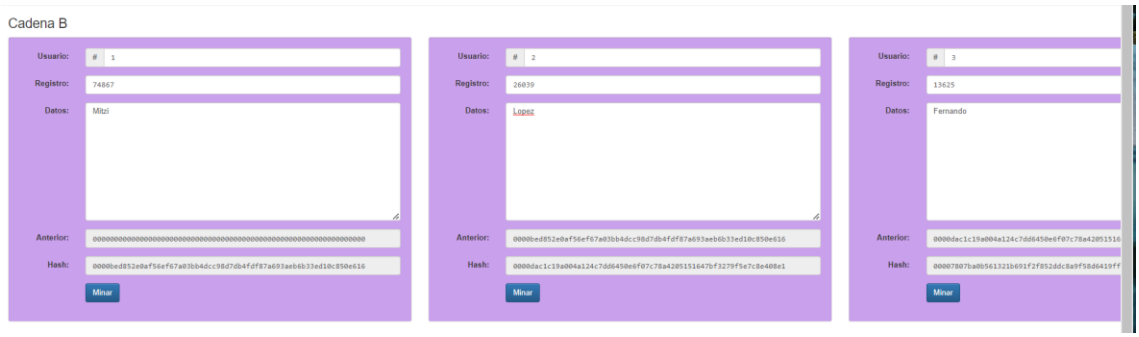


Figura 44: De la misma manera la cadena B, presente los mismos hashes en todos sus bloques, porque la información que contienen es igual.

REMIX IDE – SOLIDITY- SMART CONTRACT- ETHERSCAN

Dentro de la investigación se estableció el uso de las herramientas ya mencionadas en el título de este párrafo, que permitieron demostrar el uso back-end de un Smart contract, escrito en lenguaje solidity y que fue publicado como cadena descentralizada en ether scan.

Código de Smart contract

```
// SPDX-License-Identifier: GLP-3.0
pragma solidity ^0.8.6;

contract Blockchain{
    uint nextId;

    struct Task{
        uint id;
        string cedula;
        string nombres;
        string barrio;
    }
```

```
    Task[] tasks;

    function createTask (string memory _cedula, string memory _nombres, string
memory _barrio) public {
        tasks.push(Task(nextId, _cedula, _nombres, _barrio));
        nextId++;
    }

    function findIndex(uint _id) internal view returns (uint){
        for (uint i = 0; i < tasks.length; i++){
            if (tasks[i].id ==_id){
                return i;
            }
        }
        revert('Fue modificado');
    }

    function readTask(uint _id) public view returns (uint, string memory, string
memory, string memory){
        uint index = findIndex(_id);
        return (tasks[index].id, tasks[index].cedula, tasks[index].nombres,
tasks[index].barrio);
    }

    function updateTask(uint _id, string memory _cedula, string memory _nombres,
string memory _barrio) public{
        uint index = findIndex(_id);
        tasks[index].cedula = _cedula;
        tasks[index].nombres = _nombres;
        tasks[index].barrio = _barrio;
    }

    function deleteTask(uint _id) public{
        uint index = findIndex(_id);
        delete tasks[index];
    }
}
```

Se uso Solidity en versión 0.8.6, para la previa compilación. Además de hacer uso de la wallet Metamask para poder realizar las transacciones, dentro de la red de prueba Rinkeby, es interesante conocer que Ethereum permite realizar pruebas: para aquello da la moneda de la red conocida como ether, recordando que es la segunda cadena de bloques más grande del mundo.

Figura 45: Wallet de Metamask, valores de ether en red de prueba Rinkeby

Y además de publicar el contrato en la red de Ethereum, lo que es posible visualizar en etherscan

Figura 46: Contrato emitido y publicado en la red de Ethereum

Una vez que el contrato fue publicado, cualquier transacción realizada será vista dentro de la plataforma, además puede ser observada desde cualquier rincón con acceso a internet y etherscan.

INTERFAZ GRAFICA – INGRESO DE USUARIOS

En este punto se usó conocimientos de programación JavaScript, además de usar el entorno de visual studio, Truffle, Ganache y Metamask. Para esto la interfaz será del ingreso de usuarios y la activación de estos, mientras no este activado el usuario tendrá un nodo sin embargo no estará conectado en la cadena de bloques.

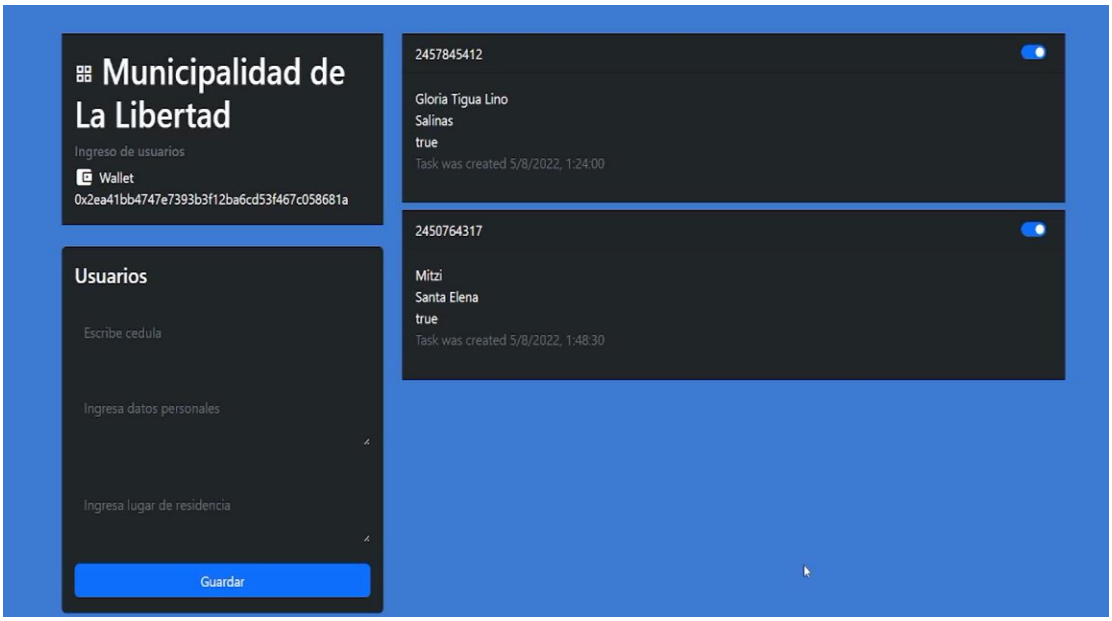


Figura 47: Los valores a ingresar son string, y solicitan: cedula, nombres completos, y lugar de residencia.

Para realizar dichas pruebas se hizo comunicación con Ganache de Ethereum que permite las pruebas y para esto da 10 cuentas con valores de 100 ETH para cada una, estas claves

privadas se vuelven cuentas en Metamask y poder realizar las transacciones correspondientes.

Cada paso establecido dentro de la parte de la creación de bloques y cadenas de bloque, fueron divididas con el fin de demostrar su usabilidad y funcionalidad en cada parte, sin embargo, en el siguiente diagrama se muestra como estaría establecida un red pública y privada, que sería de uso para la municipalidad.

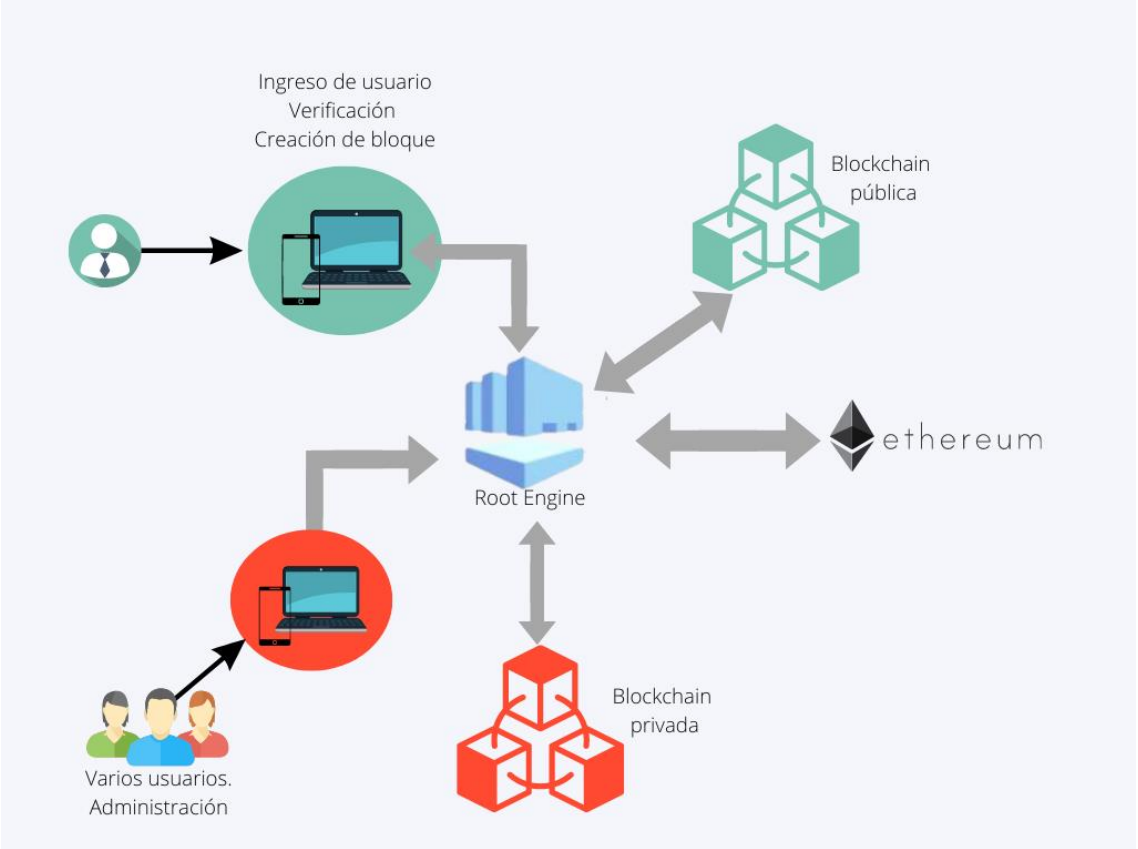


Figura 48: El diagrama demuestra como funcionaria una red compuesta privada e púbica

Estas cadenas estarían compuestas por los ciudadanos que en este caso estarían dentro de la blockchain publica, y los administradores o empleados de la municipalidad en una blockchain privada, ya que existe información que no debe ser de conocimiento público. Todo esto manejado a traves de Ethereum que permite el consenso de ambas partes y almacena uno de los mayores libros abiertos del mundo.

Las diferencias de las cadenas estan relacionadas a la descentralizacion que mantengan, según la Tabla 9, una Blockchain privada no tiene en exceso de participantes, por lo que su red suele ser mas centralizada y su acceso es reservado en el caso de los smart contract su red suele ser privada entre dos partes; una cadena de bloques publica, tiene como

principal objetivo manejar recompensas el claro ejemplo es Hyperledger, y tiende a tener problemas relacionados con escalabilidad y lentitud al procesar las transacciones. La igualdad de ambas recaen en que trabajan como libro abierto de registros, estos pueden ser añadidos, pero muy dificilmente modfificados o eliminados. En ambos casos se tiende a verificar la validez de los registros, para que los mismos sean inmutables, esto evita la manipulacion de los mismos [125].

SEGURIDAD

Figura 49: Seguridad de BD relacional y no relacional; Blockchain

Otros beneficios en lo que concierne a seguridad dentro de Blockchain son:

- Gestión de accesos e identidades
- Gestión de claves públicas y privadas
- Criptografía
- Endoso de transacción
- Integridad
- Inmutabilidad
- Disponibilidad
- Resiliencia operacional
- Eliminación de control centralizado
- Transacciones firmadas digitalmente

Entre otros que ya se mencionaron anteriormente dentro de esta investigación.

CONCLUSIONES

- Las herramientas seleccionadas en el transcurso de la investigación fueron de utilidad para poder cumplir con el objetivo de realizar el demo de blockchain, sin embargo, también se hizo uso de otras herramientas con uso en el navegador y wallet que pudieron demostrar cómo funcionaba un Smart contracts en back-end
- La reducción de los ataques cibernéticos con el uso de blockchain resultaron de manera conveniente para el investigador, ya que al usar llaves criptográficas y nonce, que son algoritmos matemáticos que permiten asegurar la información que contengan, evitando así algún cambio en los datos, ya que al ser modificados sus valores de hash y nonce se alteran.
- El uso de blockchain permite considerar los tres pilares de la seguridad que son confiabilidad, disponibilidad e integridad.
- Las cadenas de bloque se conforman por nodos que se distribuyen con la finalidad de que la información se distribuya y que no exista ningún tipo de robo. Si un nodo se cae la información que contenía queda grabada en la cadena, si alguien quiere modificar o alterarla no puede ya que un bloque creado dentro de la red jamás puede ser eliminado.
- Se realizo las tablas comparativas de las bases de datos relacionales y no relacionales, además de también comparar con las tecnologías blockchain.
- Cabe destacar que Blockchain es un campo totalmente nuevo de donde se está aprovechando los conocimientos previos sobre lenguajes como java script para poder hacer uso de las funcionalidades que tiene.

RECOMENDACIONES

- Se recomienda verificar el uso de herramientas de otras herramientas que en este trabajo no fueron utilizadas debido al coste de estas.
- Usar otras plataformas como Hyperledger, Corda Qurom para analizar las diferentes maneras de crear cadenas de bloque
- El uso de bases de datos vinculadas a Blockchain, son de utilidad en algunos centros de salud, también podrían servir para manejar la parte administrativa de un gobierno nacional.
- Se recomienda investigar mas acerca de cómo funcionan los monederos digitales al momento de crear cadenas de bloque o hacer uso de sus aplicativos

- Otra de las áreas que están muy relacionadas a blockchain es la WEB3, en función a como se manejan las interfaces de usuario a través de DaPP
- Otro de los campos pocos conocidos son los NTF que son tokens, un activo encriptado, deberían estudiarse más.

BIBLIOGRAFÍA

[1] I. Armendariz Perez, «Análisis de los principales sistemas de gestión de bases de datos ante ataques básicos,» 28 Enero 2016. [En línea]. Available: https://reunir.unir.net/bitstream/handle/123456789/3619/ARMENDARIZ%20PEREZ%2c%20I%c3%91IGO.pdf?sequence=1&isAllowed=y.

[2] M. Angel Mendoza, «Cibercrimen: 5 ataques utilizados con más frecuencia,» ESET, 14 Diciembre 2018. [En línea]. Available: https://www.welivesecurity.com/la-es/2018/12/14/cibercrimen-ataques-comunes/.

[3] Infocyte, «Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks,» 26 Marzo 2021. [En línea]. Available: https://www.infocyte.com/es/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/.

[4] D. Bravo, «Ecuador se muestra vulnerable a ciberataques,» *El Comercio*, 26 Julio 2015.

[5] France24, Reuters, EFE, «Falla informática en Ecuador: los datos de casi toda a población quedaron expuestos,» *France24*, 17 Septiembre 2019.

[6] A. Spadafora , «Canon confirms it was hit by major ransomware attack, customer data stolen,» *techradar.pro*, 27 Noviembre 2020.

[7] A. T. Norman, Todo sobre Tecnologia Blockchain, Tektime Srls, 2017.

[8] P. García Mateo, *Blockchain aplicado al sector público*, Valencia: Escola Tècnica Superior d'Enginyeria Informàtica. Universitat Politècnica de València , 2017-2018.

[9] H. Hou, *La aplicación de la tecnología Blockchain en Gobierno electrónico en China*, China: Universidad Sun Yat-Sen, 2017.

[10] J. Santiago Preisegger, R. Muñoz , A. Pasini y P. Pesado, *Blockchain y gobierno digital*, Argentina: Instituto de Investigación en Informática LIDI (III-LIDI). Facultad de Informática – Universidad Nacional de La Plata, 2019.

[11] . V. M. BALDEÓN CORONEL y J. F. ZAMBRANO HIDALGO , «IMPLEMENTACIÒN DE UN PROTOTIPO DE UNA RED DESCENTRALIZADA BLOCKCHAIN PARA EL VOTO ELECTRÓNICO EN LA UNIVERSIDAD DE GUAYAQUIL,» GUAYAQUIL, 2018.

[12] V. R. MENDIETA ALVARADO, «ANÁLISIS Y DISEÑO DE UN ARQUETIPO PARA UNA SOLUCIÓN BLOCKCHAIN ORIENTADA A LA SEGURIDAD DE LA INFORMACION DE APLICACIONES EN LINEA UTILIZADAS EN TERAPIAS

MEDICAS. CASO DE APLICABILIDAD PARA EL MODELO DE SEGURIDAD DEL DISEÑO DE LA APLICACION TEMONET,» GUAYAQUIL, 2019.

[13] N. Bauerle, «Blockchain 101,» COINDESK, 12 Noviembre 2020. [En línea]. Available: https://www.coindesk.com/learn/blockchain-101/how-does-blockchain-technology-work.

[14] Power Data, «Base de datos distribuidas de tipo blockchain,» 17 Agosto 2017. [En línea]. Available: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/base-de-datos-distribuidas-de-tipo-blockchain.

[15] Microsoft, «Microsoft: Windows 10 y los servicios en línea del usuario,» 2021. [En línea]. Available: https://privacy.microsoft.com/es-mx/windows10privacy.

[16] Postman, «Postman.org,» 2021. [En línea]. Available: https://www.postman.com/.

[17] Anaconda, «Edicion Individual,» 2021. [En línea]. Available: https://www.anaconda.com/products/individual.

[18] Anaconda, «Spyder - Documentacion de Anaconda,» [En línea]. Available: https://docs.anaconda.com/anaconda/user-guide/tasks/integration/spyder/.

[19] Microsoft, «Visual Studio Code,» [En línea].

[20] The Open JS Foundation, «Node.js,» 2022. [En línea]. Available: https://nodejs.org/es/about/.

[21] RemixIDE, «Despliegue y transacciones en Blockchain,» 2021. [En línea]. Available: https://remix-project.org/.

[22] Ganache, «Ganache - One click Blockchain,» 2021. [En línea]. Available: https://www.trufflesuite.com/ganache.

[23] MetaMask, «Metamask,» MetaMask, 2022. [En línea]. Available: https://medium.com/metamask.

[24] Facsistel Upse, «LÍNEAS DE INVESTIGACIÓN,» Facsistel UPSE, 2021. [En línea]. Available: http://facsistel.upse.edu.ec/index.php?option=com_content&view=article&id=58&Itemid=463.

[25] D. Tapscott, A. Tapscott y J. Salmerón, «Blockchain Revolution,» DEUSTO, Barcelona, 2017.

[26] C. Ortega Laurel, «U-GOB,» 01 Julio 2019. [En línea]. Available: https://u-gob.com/blockchain-para-la-administracion-publica/.

[27] C. Pastorino, «Blockchain: qué es, cómo funciona y cómo se está usando en el mercado,» WE LIVE SECURITY, 04 Septiembre 2018. [En línea]. Available: https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/.

[28] Gobierno del Ecuador , «Sistema de Información para los Gobiernos Autónomos Descentralizados,» 2021. [En línea]. Available:

https://www.planificacion.gob.ec/sistema-de-informacion-para-los-gobiernos-autonomos-descentralizados/.

[29] BINANCE ACADEMY, «¿Qué hace que una Blockchain sea segura?,» 19 Marzo 2019. [En línea]. Available: https://academy.binance.com/es/articles/what-makes-a-blockchain-secure.

[30] Secretaria Nacional de Planificación- ECUADOR, PLAN DE CREACIÓN DE OPORTUNIDADES 2021-2025, Quito: Secretaria Nacional de Planificación, 2021.

[31] P. I. L. Velazques Araque PhD, Metologias de la investigacion, vol. 1, 2010, pp. 1-5.

[32] L. R. Gay, «Educational Research Neu Jersey,» Estados Unidos , Prentice Hall Inc., 1996.

[33] D. R. Hernandez Sampieri, D. C. Fernandez Collado y D. M. d. P. Baptista Lucio, Metodología de la Investigación, Mexico: Mc Graw Hill, 2014.

[34] Gobierno de Mexico, «La importancia de las bases de datos,» 26 Junio 2017. [En línea]. Available: https://www.inecol.mx/inecol/index.php/es/2017-06-26-16-35-48/17-ciencia-hoy/1426-la-importancia-de-las-bases-de-datos.

[35] BBC News Mundo, «"Estamos en guerra": 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia,» 20 Mayo 2022. [En línea]. Available: https://www.bbc.com/mundo/noticias-america-latina-61516874.

[36] E. MÜLLER, «Alemania sufre el mayor ‘hackeo’ de su historia con la filtración de datos personales de centenares de políticos,» *EL PAÍS*, 04 Enero 2019.

[37] L. Benítez Eyzaguirre, «Blockchain para la transparencia, gestión pública y colaboración1,» *Teknokultura. Revista de Cultura Digital y Movimientos Sociales*, 2020.

[38] CEPAL - Naciones Unidas, «Gobiernos Autónomos Descentralizados de Ecuador,» Observatorio Regional de Planificacion para el desarrollo de América y el Caribe, [En línea]. Available: https://observatorioplanificacion.cepal.org/es/instituciones/gobiernos-autonomos-descentralizados-de-ecuador.

[39] Gobierno del Encuentro. Ecuador, «Los GAD son instancias cruciales para la garantía de derechos,» Consejo Nacional para la Igualdad Intergeneracional, 2022. [En línea]. Available: https://www.igualdad.gob.ec/los-gad-son-instancias-cruciales-para-la-garantia-de-derechos/.

[40] Consejo Nacional de Competencias, «SISTEMA NACIONAL DE COMPETENCIAS,» 2019. [En línea]. Available: http://www.congope.gob.ec/wp-content/uploads/2019/01/PRESENTACIO%CC%81N-CANDIDATOS_GUAYAQUIL.pptx#:~:text=y%2042%20Cootad-,Planificar%2C%20regular%20y%20controlar%20el%20tr%C3%A1nsito%20y%20el%20transporte%20terrestre,y%20contribuciones%20especiales%20de%.

[41] Asamblea Nacional, «CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR,» Quito, Ecuador .

[42] Asamblea Constitucional de la República del Ecuador, «CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP,» 2021.

[43] M. A. GUITIERREZ DIAZ, «BASES DE DATOS,» [En línea]. Available: https://www.aiu.edu/cursos/base%20de%20datos/pdf%20leccion%201/lecci%C3%B3n%201.pdf.

[44] IntelDig, «Bases de Datos: Tipos, Usos y Beneficios,» Tecnologias Informacion, 2018. [En línea]. Available: https://www.tecnologias-informacion.com/basesdedatos.html.

[45] J. Ramos Martín , A. Ramos Martín y F. Montero Rodríguez, SISTEMAS GESTORES DE BASES DE DATOS, . Á. Rodríguez Luengo, Ed., Madrid: Mc Graw Hill, 2006.

[46] MySQL, «¿Por qué MySQL?,» MySQL.com, 2021. [En línea]. Available: https://www.mysql.com/why-mysql/.

[47] postgresql.org, «Acerca de PostgreSQL,» 2021. [En línea]. Available: https://www.postgresql.org/about/.

[48] M. Parada, «Qué es SQL Server,» OpenWebinars, 23 Noviembre 2019. [En línea]. Available: https://openwebinars.net/blog/que-es-sql-server/.

[49] Amazon AWS, «¿Qué es NoSQL?,» AWS, 2021. [En línea]. Available: https://aws.amazon.com/es/nosql/.

[50] MongoDB, «La base de datos líder para aplicaciones modernas,» MongoDB, 2021. [En línea]. Available: https://www.mongodb.com/es.

[51] redis.io, «REDIS,» REDISlab, 2021. [En línea]. Available: https://redis.io/.

[52] Cassandra Documentation, «Apache Cassandra,» 2022. [En línea]. Available: https://cassandra.apache.org/doc/latest/cassandra/new/index.html.

[53] J. M. Alonso Cebrián, V. Díaz Sáez, A. Guzmán Sacristán, P. Laguna Durán y A. Martín Bailon, «Seguridad en las bases de datos,» FUOC, Barcelona, 2012.

[54] F. Medina Lopez, «Módulo 9. Seguridad en Base de Datos,» COAPA.

[55] Power Data, «Seguridad de datos: En qué consiste y qué es importante en tu empresa,» Power Data, 2021. [En línea]. Available: https://www.powerdata.es/seguridad-de-datos.

[56] Business Insider, «10 grandes amenazas de bases de datos,» 2021, [En línea]. Available: https://www.businessinsider.es/buscar?keys=10%20grandes%20amenazas%20seguridad%20bases%20datos&page=1.

[57] Imperva, «Top 5 Database Security Threats,» 2016.

[58] IMPERVA, «Las diez principales amenazas para las bases de datos,» Imperva, 2020. [En línea]. Available: https://www.imperva.com/.

[59] Mitre Corporation, «CVE,» 2022. [En línea]. Available: https://www.cve.org/About/Overview.

[60] CVE MITRE CORPORATION, «CVE-2022-31026,» CVE List, 2022. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31026.

[61] CVE MITRE CORPORATION, «CVE-2022-21490,» CVE List, 2022. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21490.

[62] CVE MITRE CORPORATION, «CVE-2021-42662,» CVE List, 2022. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42662.

[63] CVE MITRE CORPORATION, «CVE-2022-21460,» CVE List, 2021. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21460.

[64] CVE MITRE CORPORATION, «CVE-2013-0255,» CVE List, 2013. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0255.

[65] CVE MITRE CORPORATION, «CVE-2009-4136,» CVE List|, 2009. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4136.

[66] CVE MITRE CORPORATION, «CVE-2009-4034,» CVE List, 2009. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4034.

[67] CVE MITRE CORPORATION, «CVE-2009-3231,» CVE List, 2009. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3231.

[68] CVE MITRE CORPORATION, «CVE-2022-30335,» CVE List, 2022. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30335.

[69] CVE MITRE CORPORATION, «CVE-2021-38159,» CVE List, 2021. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38159.

[70] CVE MITRE CORPORATION, «CVE-2021-25275,» CVE List, 2021. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25275.

[71] CVE MITRE CORPORATION, «CVE-2020-1455,» CVE List, 2020. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1455.

[72] CVE MITRE CORPORATION, «CVE-2022-24272,» CVE List, 2022. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24272.

[73] CVE MITRE CORPORATION, «CVE-2021-32040,» CVE List, 2021. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32040.

[74] CVE MITRE CORPORATION, «CVE-2021-32039,» CVE List, 2021. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32039.

[75] CVE MITRE CORPORATION, «CVE-2021-20334,» CVE List, 2021. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20334.

[76] CVE MITRE CORPORATION, «CVE-2022-0543,» CVE List, 2022. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0543.

[77] CVE MITRE CORPORATION, «CVE-2021-33026,» CVE List, 2021. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33026.

[78] CVE MITRE CORPORATION, «CVE-2021-31649,» CVE List, 2021. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31649.

[79] CVE MITRE CORPORATION, «CVE-2021-29469,» CVE List, 2021. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29469.

[80] CVE MITRE CORPORATION, «CVE-2021-44521,» CVE List, 2021. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44521.

[81] CVE MITRE CORPORATION, «CVE-2021.40525,» CVE List, 2021. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40525.

[82] CVE MITRE CORPORATION, «CVE-2020-13946,» CVE List, 2020. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13946.

[83] CVE MITRE CORPORATION, «CVE-2019-16869,» CVE List, 2019. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16869.

[84] T. Foltýn, «NASA sufrió brecha de seguridad y robaron información sobre la misión a Marte,» 25 Junio 2019. [En línea]. Available: https://www.welivesecurity.com/la-es/2019/06/25/nasa-sufrio-brecha-de-seguridad-y-robaron-informacion-sobre-la-mision-a-marte/.

[85] Periódico: Semana, «‘Hackearon’ al DANE: la entidad confirmó que fue víctima de un ataque informático desde la medianoche del martes,» Semana, Colombia, 2021.

[86] J. M. Harán, «Banco Pichincha sufrió ataque informático que afectó parte de sus servicios,» WeliveSecurity, Octubre 2021. [En línea]. Available: https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/.

[87] G. Pérez, «El Ministerio de Trabajo y Economía Social sufre un ciberataque,» El País, 09 Junio 2021. [En línea]. Available: https://elpais.com/economia/2021-06-09/el-ministerio-de-trabajo-y-economia-social-sufre-un-ciberataque.html.

[88] N. Dávalos, «Los misterios del ataque que dejo a CNT sumida en la "emergencia",» Primicias , Quito, 2021.

[89] W. Walker , Blockchain: Aplicaciones y Entendiento en el mundo real, Estados Unidos, 2018.

[90] J. Segura, «Tecnología Blockchain: qué es y cómo funciona,» Estratega financiero, 2020. [En línea]. Available: https://estrategafinanciero.com/tecnologia-blockchain-funciona/.

[91] A. Preukschat, C. Kuchkovsky, G. Gómez Lardies, D. Díez y Í. Molero, «Blockchain: la revolución industrial de internet,» Centro Libros PAPF, S. L. U., Barcelona, 2017.

[92] TECH ECUADOR, «Caracteristicas del Blockchain,» TECH ECUADOR. Facultad de informática, 01 Marzo 2021. [En línea]. Available: https://www.techtitute.com/ingenieria/blog/las-caracteristicas-del-blockchain.

[93] S. Abeyratne y R. Monfared, «BLOCKCHAIN READY MANUFACTURING SUPPLY CHAIN USING DISTRIBUTED LEDGER,» *IJRET: International Journal of Research in Engineering and Technology,* vol. 05, 2016.

[94] S. Bogart y K. Rice, «The Blockchain Report: Welcome to the Internet of Value,» *Needham,* pp. 1-57, 2015.

[95] Tokens24, «Aspectos, problemas y limitaciones de Blockchain,» Team Tokens 24, 12 Mayo 2018. [En línea]. Available: https://www.tokens24.com/es/cryptopedia/basics/problemas-limitaciones-y-problemas-de-blockchain.

[96] Adiat.org, «17 APLICACIONES DE LA TECNOLOGÍA BLOCKCHAIN,» Adiat, 2021. [En línea]. Available: http://adiat.org/17-aplicaciones-de-la-tecnologia-blockchain#page-content.

[97] SERMAN, «Blockchain: El futuro del almacenamiento tiende a la fragmentación,» 2021. [En línea]. Available: https://serman.com/.

[98] C. García Moreno, «Gestión de la identidad digital a través de Blockchain,» INDRA, 2021. [En línea]. Available: https://www.indracompany.com/es/blogneo/gestion-identidad-digital-traves-blockchain.

[99] IBM, «¿Qué son los contratos inteligentes en blockchain?,» IBM, 2022. [En línea]. Available: https://www.ibm.com/topics/smart-contracts.

[100] N. Rodriguez, «Blockchain Para La Cadena De Suministro: El Cambio En El Juego,» 101 Blockchains, 30 Junio 2019. [En línea]. Available: https://101blockchains.com/es/blockchain-para-la-cadena-de-suministro/#1.

[101] J. Ibáñez Jiménez, «Blockchain, ¿el nuevo notario?,» Everyis / NTT DATA Company, España.

[102] SAFEBOX , «CÓMO LA TECNOLOGÍA BLOCKCHAIN BENEFICIA LA ENOTARIZATION,» SAFEBOX , 2020. [En línea]. Available: https://safeboxsigning.com/como-la-tecnologia-blockchain-beneficia-la-enotarization/.

[103] Ethereum.org, «Ethereum,» 2021. [En línea]. Available: https://ethereum.org/en/.

[104] B. Villegas Martín, «BLOCKCHAIN Y SU APORTACIÓN A LA CIUDAD INTELIGENTE,» Universidad Politécnica de Madrid, Madrid, 2022.

[105] NRC.Canada, «Explorando blockchain para mejores negocios,» Consejo Nacional de Investigación de Canadá, 20 Agosto 2018. [En línea]. Available: https://nrc.canada.ca/en/stories/exploring-blockchain-better-business.

[106] N. Leal, «Canada pilots blockchain staff records,» Global Government forum, 17 Junio 2019. [En línea]. Available: https://www.globalgovernmentforum.com/canada-pilots-blockchain-staff-records/.

[107] «Vicente Fox de México invita a la comunidad blockchain a unirse a su "revolución amarilla",» *Revista Bitcoin*, 2018.

[108] Departamento de Defensa. United States of America, «DoD DIGITAL MODERNIZATION STRATEGY,» 12 Julio 2019. [En línea]. Available: https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.

[109] BBC News Mundo, «Bitcoin: El Salvador se convierte este martes en el primer país del mundo en adoptar la criptomoneda como divisa de curso legal,» 7 Septiembre 2021. [En línea]. Available: https://www.bbc.com/mundo/noticias-america-latina-58441561.

[110] EL UNIVERSO, «71% de cuentas de dinero electrónico, sin uso en Ecuador,» *EL UNIVERSO,* 03 Diciembre 2017.

[111] «NEC, IDB Lab and NGO Bitcoin Argentina to Deploy a Blockchain-ba,» JCN Newswire, 25 Agosto 2019. [En línea]. Available: https://www.bloomberg.com/press-releases/2019-08-26/nec-idb-lab-and-ngo-bitcoin-argentina-to-deploy-a-blockchain-ba.

[112] S. Sundararajan, «El gobierno austriaco respalda el nuevo instituto de investigación Blockchain,» 07 Diciembre 2017. [En línea]. Available: https://www.coindesk.com/austrian-government-backs-new-blockchain-research-institute.

[113] e-estonia, «e-Estonia Briefing Center,» e-estonia, 2021. [En línea]. Available: https://e-estonia.com/solutions/security-and-safety/.

[114] «L'Ajuntament de Valls presenta el projecte del Portal de Dades Municipal,» *Tarragonadigital,* 20 Septiembre 2019.

[115] I. Allison, «Bitland está revolucionando el registro de tierras africano en asociación con CCEDK,» *International Business Times,* 31 Agosto 2016.

[116] A. Damana y M. Ford, «South African National Blockchain Alliance,» CSIR, Sudafrica, 2018.

[117] F. Ng'wanakilala, «Tanzania dice que más de 10,000 'trabajadores fantasmas' fueron eliminados de la nómina del gobierno,» *REUTERS,* 16 Mayo 2016.

[118] Wechat oficial de Chain World, «Decodificando los genes blockchain de las ciudades digitales,» Wechat oficial de Chain World, 22 Noviembre 2019. [En línea]. Available: https://mp.weixin.qq.com/s/lBE4y9VQw81uwxSuslFitg.

[119] W. Zhao, «El gobierno coreano liderará 6 pilotos de blockchain con un fondo de $ 9 millones,» Coin Desk, 22 Junio 2018. [En línea]. Available: https://www.coindesk.com/korean-government-lead-6-blockchain-pilots-9-million-fund.

[120] F. Serale, C. Redl y A. Muente Kunigami, «BLOCKCHAIN EN LA ADMINISTRACIÓN PÚBLICA ¿Mucho ruido y pocos bloques?,» 2019. [En línea]. Available: https://publications.iadb.org/publications/spanish/document/Blockchain_en_la_administraci%C3%B3n_p%C3%BAblica_Mucho_ruido_y_pocos_bloques_es.pdf.

[121] M. Barrón Bastida, E. de la Torre Romero y B. Hernández Sánchez, «Estudio exploratorio sobre la tecnología blockchain aplicada en cadenas de suministro,» Instituto Mexicano del Transporte, Mexico, 2020.

[122] M. Cordero Valdavida, «BLOCKCHAIN EN EL SECTOR PÚBLICO, UNA PERSPECTIVA INTERNACIONAL,» Tribunal de Cuentas Europeo, 2019.

[123] C. A. CARRILLO VILLALVA, «"DISEÑO Y APLICACIÓN DE UN SISTEMA DE SEGURIDAD DESCENTRALIZADO MEDIANTE LA TECNOLOGÍA BLOCKCHAIN PARA APLICACIONES WEB",» ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO, Riobamba - Ecuador, 2021.

[124] I. Pérez, «Blockchain: bloques, transacciones, firmas digitales y hashes,» Criptonoticias, 2020. [En línea]. Available: https://www.criptonoticias.com/criptopedia/blockchain-bloques-transacciones-firmas-digitales-hashes/#Propiedades_de_una_funcion_hash_segura.

[125] A. Kapoor, «Blockchain Público Vs. Privado: Una Comparación Exhaustiva,» Blockchain Council.org, 2022. [En línea]. Available: https://www.blockchain-council.org/blockchain/blockchain-publico-vs-privado-una-comparacion-exhaustiva/#:~:text=Diferencias%20entre%20Blockchains%20P%C3%BAblicos%20y%20Privados&text=En%20blockchains%20privados%2C%20s%C3%B3lo%20las,Ejemplos%3A%20Hyperledge.

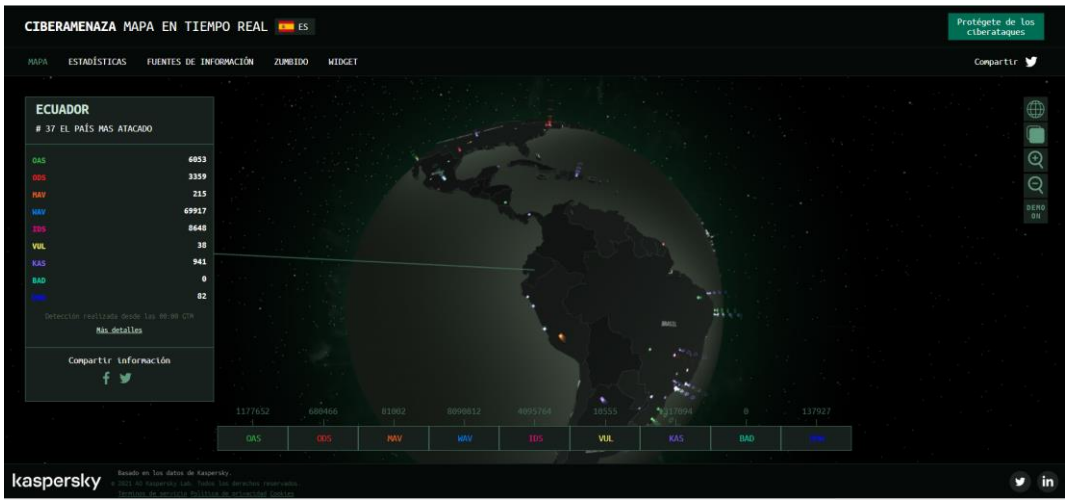
[126] MEW, «Ethereum's Original Wallet,» 2021. [En línea]. Available: https://www.myetherwallet.com.

[127] MYSQL, © 2022 Oracle, [En línea]. Available: https://www.mysql.com/why-mysql/.

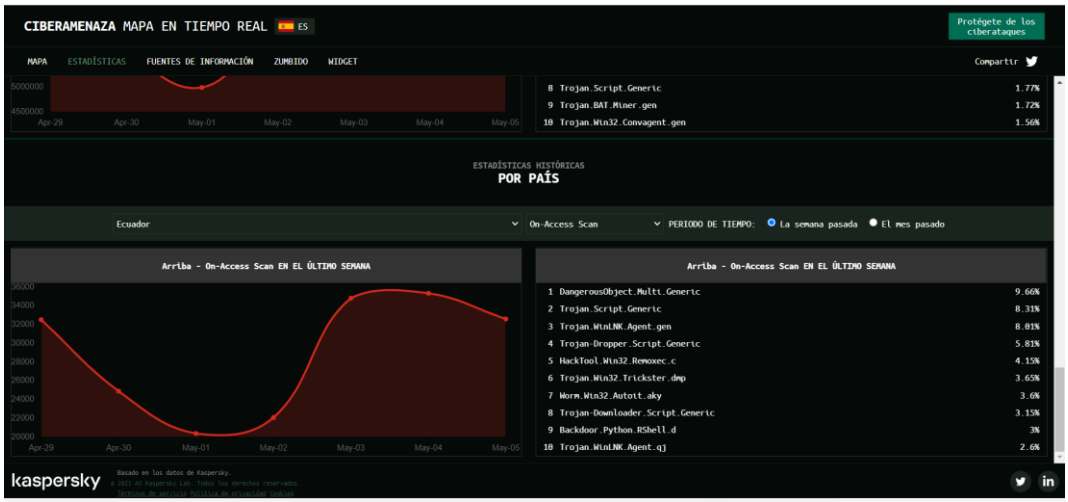
[128] MongoDB, Inc., «MongoDB, Inc.,» MongoDB, Inc., 2022. [En línea]. Available: https://www.mongodb.com/es/what-is-mongodb.

[129] Q. SHANG y A. PRICE, «Blockchain for Global Development II,» 2021. [En línea]. Available: https://watermark.silverchair.com/inov_a_00276.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAAqIwggKeBgkqhkiG9w0BBwagggKPMIICiwIBADCCAoQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMSRFfjI98BbW3ZLyfAgEQgIICVYxwJWxdnnUa1Gwdcv4F0M8Rq6jsCqrTlGVZBVNvaB.

ANEXOS



Anexo 1: Ecuador, ubicado en el puesto #37.



Anexo 2: Lista de ataques realizados en tiempo real

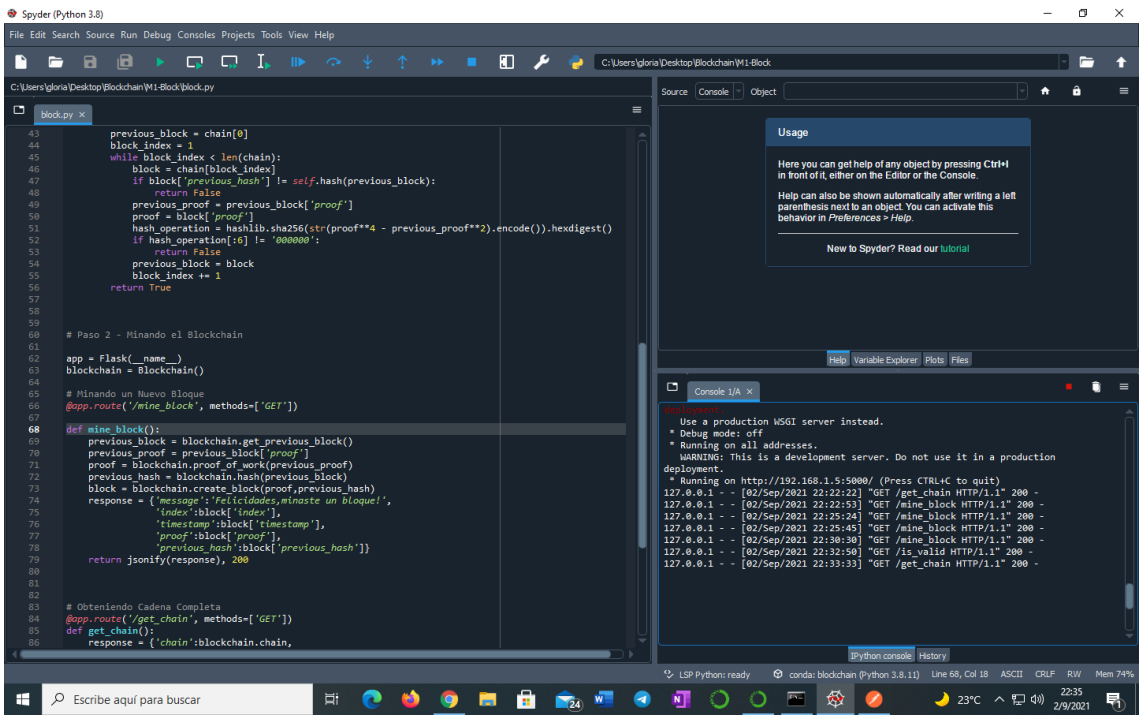
Universidad Estatal Península de Santa Elena

Carrera de Tecnologías de la Información

Nombre del entrevistador	Mitzi Saquicela Tigua	Duración	1 hora
Tema	Análisis de vulnerabilidades en técnicas tradicionales de almacenamiento vs tecnologías de blockchain en entidades gubernamentales. CASO DE ESTUDIO: MUNICIPALIDAD DE LA PROVINCIA DE SANTA ELENA		

- ¿El municipio está preparado para un ataque?
- ¿Cuentan con protocolos de seguridad informática?
- ¿De qué manera crean respaldos de la información (o sea si usan raid o backup)?
- ¿Quiénes pueden acceder al centro de datos? en caso de tener uno
- ¿Entiende el termino SQL INYECTION?
- ¿Conoce el termino de DDOS?
- ¿Tiene un software antivirus instalado en las pc de su departamento?
- ¿Quiénes tienen acceso a modificar, actualizar, o revisar las bases de datos?
- ¿Tiene contraseñas para el acceso a las bases de datos?
- ¿Se puede acceder a las bases de datos fuera del horario laboral?
- ¿Qué entiende por cadena de bloques?
- ¿Ha escuchado acerca de las bases de datos distribuidas?

Anexo3: Entrevista.



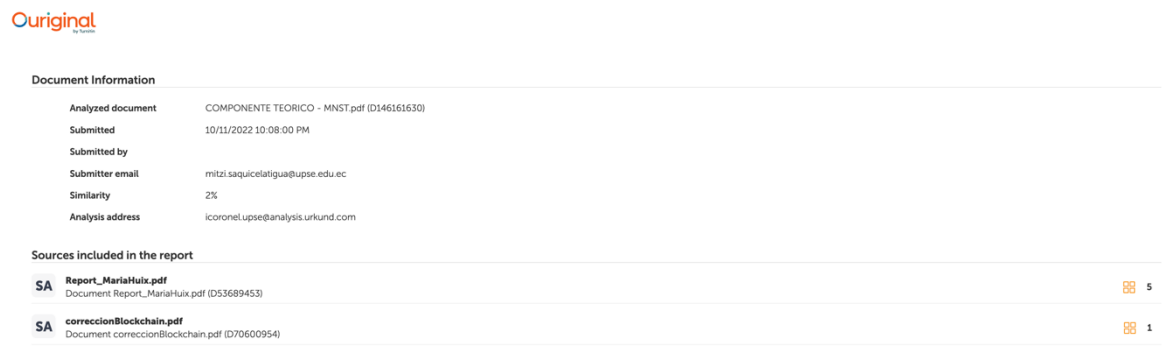
Anexo 4: Uso de Anaconda y e lenguaje de Python para la creación de la cadena de bloque

La Libertad, 11 de octubre de 2022

CERTIFICADO ANTIPLAGIO

002-TUTOR IACS-2022

En calidad de tutor del trabajo de titulación denominado **"VULNERABILIDADES EXISTENTES EN TÉCNICAS TRADICIONALES DE ALMACENAMIENTOS DE DATOS VS TECNOLOGÍAS EMERGENTES COMO BLOCKCHAIN EN ENTIDADES GUBERNAMENTALES"**, elaborado por la estudiante, **SAQUICELA TIGUA MITZI NOEMI**, egresada de la Carrera de Tecnologías de la Información, de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniera en Tecnologías de la Información, me permito declarar que una vez analizado en el sistema antiplagio URKUND, luego de haber cumplido los requerimientos exigidos de valoración, el presente proyecto ejecutado, se encuentra con 2% de la valoración permitida, por consiguiente se procede a emitir el presente informe.



Ouriginal

Document Information

Analyzed document	COMPONENTE TEORICO - MNST.pdf (D146161630)
Submitted	10/11/2022 10:08:00 PM
Submitted by	
Submitter email	mitzi.saquicelatigua@upse.edu.ec
Similarity	2%
Analysis address	icoronel.upse@analysis.urkund.com

Sources included in the report

SA	**Report_MariaHuix.pdf** Document Report_MariaHuix.pdf (D53689453)	5
SA	**correccionBlockchain.pdf** Document correccionBlockchain.pdf (D70600954)	1

Atentamente,

Ing. Coronel Suárez Iván Alberto, MSIA.
C.I.:0917255978
DOCENTE TUTOR