

Información General			
Facultad: CIENCIAS NATURALES E INGENIERIA			
Programa académico: INGENIERIA DE TELECOMUNICACIONES		Grupo(s) de investigación: GNET	
Nombre del semillero – Siglas Semillero de Sistemas de Telecomunicaciones – SISTEL		Fecha creación: 12 de Febrero de 2015	
		Campus:	
Líneas de Investigación:			
Áreas del saber *			
	1. Agronomía veterinaria y afines		5. Ciencias sociales y humanas
	2. Bellas artes		6. Economía, administración, contaduría y afines
	3. Ciencias de la educación		7. Matemáticas y ciencias naturales
	4. Ciencias de la salud	X	8. Ingenierías, arquitectura, urbanismo y afines

Al diligenciar este documento autorizo a UNIDADES TECNOLÓGICAS DE SANTANDER, ubicada en Calle de los estudiantes 9-82 Ciudadela Real de Minas y con teléfono de contacto 6076917700, para que recolecte, almacene, use, circule y/o suprima mis datos personales. Lo anterior para dar cumplimiento a las finalidades incorporadas en la Política de Tratamiento de Información disponible en www.uts.edu.co, la cual declaro conocer y saber que en esta se especifican cuáles datos son sensibles. Así mismo, conozco que como titular me asisten los derechos a conocer, actualizar, rectificar y suprimir mis datos y revocar la autorización. Igualmente declaro que poseo autorización, de los otros titulares de datos que suministro, para que UNIDADES TECNOLÓGICAS DE SANTANDER les dé tratamiento conforme a las finalidades consignadas en la Política.

Información del Director del Proyecto

Nombre: JOHAN LEANDRO TELLEZ GARZON		No. de identificación:	
Nivel de formación académica (Pregrado / Postgrado / Link de CvLAC):			Asesor
		X	Líder de Semillero de Investigación
Correo electrónico:			

Información de los autores

Nombre	No. Identificación	Correo electrónico
Madwin Leonardo Zapata Palacio		
Elkin Yesid Ortega Sanabria		

Proyecto

1. Título del proyecto: Estudio de Factibilidad Técnica para la Implementación de Tecnología Blockchain en Telefonía IP: Caso de Uso en el Sector de las Telecomunicaciones	MODALIDAD DEL PROYECTO **				
	PA	PI	TI	RE	Otra. ¿Cuál?
			X		
Fecha creación del proyecto:				3 de septiembre de 2024	
2. Planteamiento de la problemática:					
La problemática que se pretende abordar en este trabajo de grado radica en la falta de seguridad y privacidad en las comunicaciones telefónicas a través de telefonía IP. En general no es displicente saber acerca de los riesgos que se					
ELABORADO POR: Investigación		REVISADO POR: Sistema Integrado de Gestión		APROBADO POR: Líder Sistema Integrado de Gestión FECHA APROBACIÓN: Febrero de 2025	

corren con los servicios telemáticos como lo es el uso de la telefonía IP, que presenta vulnerabilidades que pueden ser explotadas por actores malintencionados para interceptar llamadas, comprometer la integridad de los datos transmitidos y comprometer la privacidad de los usuarios. Esta situación es especialmente preocupante en un entorno donde la telefonía IP se utiliza de manera generalizada para realizar comunicaciones empresariales y personales. Pues esto conlleva a que terceros no autorizados puedan acceder al servidor de telefonía IP, otorgándoles facultad de poder secuestrar troncales telefónicas, modificar archivos de configuración y generar llamadas a otros países.

Las causas de esta problemática incluyen la falta de medidas adecuadas de seguridad y cifrado en los protocolos de telefonía IP, así como la falta de mecanismos efectivos para proteger contra la interceptación de llamadas y el espionaje.

Guerrón Subía, L. I. (2021) en su Modelo de seguridad sobre la telefonía IP/OPEN source nos asegura que la mayoría de las empresas tanto públicas como privadas, están sujetas a múltiples amenazas que pueden afectar sus activos económicos, tecnológicos, sociales y legales. Estos riesgos se intensifican cuando se trata de manejar información sensible durante conversaciones telefónicas privadas, particularmente en servicios de telefonía IP (p. 23).

La pregunta que sustenta esta problemática es: ¿Cómo la implementación de tecnología blockchain en sistemas de telefonía IP puede mejorar la seguridad, privacidad y eficiencia de las comunicaciones telefónicas ?.

3. Antecedentes: E

En 2018, en la Universidad de las Américas en Quito, se realizó un trabajo de titulación llamado: "Análisis de la utilización de la Tecnología Blockchain para la gestión de la información en Sistemas de Alarmas Residenciales". Este proyecto, desarrollado por A. K. Carrión Basantes, exploró el potencial de la tecnología blockchain, específicamente la plataforma descentralizada Ethereum, para la gestión de información en sistemas de alarmas residenciales.

La fase teórica del proyecto aborda las características fundamentales de la cadena de bloques, algoritmos de consenso, plataformas y aplicaciones descentralizadas sobre la red peer-to-peer. Se contextualiza el avance y la evolución de los sistemas de alarmas, estableciendo un marco comparativo entre los sistemas centralizados tradicionales y el nuevo enfoque descentralizado basado en blockchain. Aunque no se desarrolla ni implementa un prototipo, se simula la red peer-to-peer utilizando la plataforma Ethereum basada en el estándar ERC20. Esta simulación proporciona una visión práctica de cómo podría funcionar un sistema de alarmas residenciales basado en blockchain. Finalmente, el estudio concluye con recomendaciones y reflexiones que pueden servir como punto de partida para investigaciones futuras en el ámbito de los sistemas descentralizados de seguridad residencial.

Este proyecto aporta una perspectiva innovadora sobre el uso de la tecnología blockchain en la gestión de sistemas de alarmas residenciales, destacando su potencial para mejorar la seguridad y eficiencia de estos sistemas sin depender de intermediarios. Además, sienta las bases para investigaciones futuras en este campo emergente.

En la Universidad de las Américas, en Quito, durante el año 2020, se llevó a cabo la tesis de grado de E. A. Rodríguez Espinoza titulada "Estudio de la tecnología Blockchain para el aseguramiento de los dispositivos IoT". Este estudio se centra en explorar las posibilidades que la tecnología blockchain ofrece para garantizar la seguridad de los dispositivos IoT. La cadena de bloques, asegurada criptográficamente, permite almacenar registros únicos y distribuirlos en la red de manera consensuada, garantizando la integridad y disponibilidad de los datos transmitidos. Para lograr este objetivo, Rodríguez Espinoza realiza un estudio exhaustivo del funcionamiento y características tanto de IoT como de la tecnología blockchain. Esto proporciona una comprensión clara de los escenarios realistas en los que la encriptación blockchain puede ser funcional para asegurar dispositivos IoT. Como resultado, se proponen modelos funcionales y aplicables que permiten una transmisión segura de datos, sentando las bases para futuras aplicaciones en este ámbito. Esta investigación contribuye al avance del conocimiento en el campo de la seguridad de dispositivos IoT y destaca el papel fundamental que la tecnología blockchain puede desempeñar en este ámbito. Además, proporciona una base sólida para futuros estudios y aplicaciones en el campo de la seguridad de IoT.

En el año 2020, En Lima, se realizó una investigación en la Universidad Privada del Norte titulada "Análisis del servicio telefonía VoIP siguiendo los estándares de seguridad informática. Una revisión de la literatura científica", llevada a cabo por R. J. Briceño Gómez Sánchez. La tesis se enfoca en explorar los estándares de seguridad en la telefonía VoIP y su aplicación en el ámbito empresarial. Mediante una revisión exhaustiva de la literatura científica, el autor examina los desafíos de seguridad que enfrentan los sistemas de telefonía VoIP y propone recomendaciones basadas en estándares de seguridad informática. Este estudio proporciona una visión integral de las vulnerabilidades y amenazas en la telefonía VoIP, así como las mejores prácticas para mitigar riesgos y fortalecer la seguridad en las comunicaciones empresariales. La investigación presenta una oportunidad invaluable para comprender el estado actual de la seguridad en la telefonía VoIP y aprovechar los hallazgos y recomendaciones para enriquecer y respaldar el estudio de factibilidad técnica de la implementación de tecnología blockchain en sistemas de telefonía IP en la presente investigación.

En el año 2021, se publicó el artículo "Telecomunicaciones: de la revolución de datos a la revolución blockchain" de C. Steck y E. F. Garrido, en el libro Blockchain: la revolución industrial de internet (pp. 50-56), editado por Gestión 2000. Este trabajo explora cómo la tecnología blockchain está revolucionando el sector de las telecomunicaciones, proporcionando un análisis detallado de su impacto en diversos aspectos de la industria. En el panorama actual de las telecomunicaciones, la tecnología blockchain emerge como un factor disruptivo con el potencial de transformar profundamente diversos aspectos de esta industria. En el artículo "Telecomunicaciones: de la revolución de datos a la revolución blockchain" de Steck y Garrido (2021), se analiza detalladamente cómo la adopción de blockchain está generando nuevos modelos de negocio y afectando la gestión interna de las redes, la administración empresarial, la provisión de servicios y las barreras de entrada en este sector. el artículo de Steck y Garrido ofrece una visión integral de cómo la tecnología blockchain está transformando las telecomunicaciones, sugiriendo posibles impactos y oportunidades, Estas tendencias son relevantes para el contexto de este estudio, ya que sugieren posibles impactos y oportunidades para la investigación propuesta.

En el año 2021, en la Universidad Siglo XXI, Ariel F. L. Carrizo Saavedra presentó su Trabajo Final de Graduación titulado Ventajas competitivas del uso de Tecnología Blockchain en el sector Telecomunicaciones de Argentina para el período 2021-2025. En esta investigación, Carrizo Saavedra explora las expectativas y el estado actual del uso de la tecnología blockchain en la industria de las telecomunicaciones en Argentina, enfocándose en el período 2021-2025. La tecnología blockchain ha evolucionado significativamente desde su concepción como la infraestructura subyacente de las criptomonedas. A medida que ha madurado, ha demostrado ser mucho más que una simple base de datos compartida y segura, extendiéndose desde el ámbito informático hasta el empresarial e industrial. Su capacidad para proporcionar confianza, seguridad, transparencia, eficiencia y reducción de costos operativos la convierte en una herramienta poderosa para redefinir procesos en una amplia variedad de sectores.

El Trabajo Final de Graduación de Ariel F. L. Carrizo Saavedra se centra en investigar las expectativas y el estado actual del uso de la tecnología blockchain en la industria de las telecomunicaciones en Argentina para el período 2021-2025. Para ello, se utilizaron entrevistas con directivos de empresas y consultores de telecomunicaciones, así como datos de mercado, encuestas y aportaciones de otros autores en el campo. El estudio generó un modelo teórico que abarca conceptos iniciales sobre la tecnología blockchain, casos de uso relevantes, proyectos actuales, nuevos negocios emergentes, legislación existente y limitaciones, así como las posibles ventajas competitivas y el valor agregado que esta tecnología puede ofrecer en el sector de las telecomunicaciones en Argentina.

En el año 2022, en el Instituto Tecnológico de Buenos Aires – ITBA, María C. Cavagna presentó su tesis titulada Análisis de factibilidad del uso de la tecnología blockchain para la trazabilidad de medicamentos en Argentina. La tesis se centró en investigar cómo todo el potencial que tiene la tecnología blockchain podría ayudar a mejorar la seguridad y confiabilidad en el seguimiento y verificación de los medicamentos que se liberan al mercado, desde su elaboración hasta su dispensación. Cavagna realizó un análisis detallado donde explora las características propias de la blockchain, tales como hashes criptográficos, cifrado asimétrico y las redes de nodos P2P (peer to peer), y cómo estas pueden superar las deficiencias de los métodos tradicionales utilizados en Argentina. Este estudio recalca la capacidad del blockchain para realizar transacciones seguras y rápidas sin la necesidad de terceros. Esta investigación proporciona una valiosa perspectiva para entender las aplicaciones prácticas de la blockchain y ofrece conocimientos clave que pueden ser adaptados y aplicados al estudio de factibilidad técnica de la implementación de tecnología blockchain en sistemas de telefonía IP.

En 2022, en la revista Intelligent Automation & Soft Computing, el artículo titulado "Bcvop2p: Esquema de Autenticación Descentralizado Basado en Blockchain para Comunicación de Voz Segura", escrito por M. Kara, M. Aydın y H. H. Balık, sugiere un esquema de autenticación basado en blockchain para aplicaciones de VoIP, abordando las preocupaciones de seguridad relacionadas con las comunicaciones por Internet. Los tres autores destacan cómo la arquitectura distribuida de blockchain puede superar las limitaciones de los métodos tradicionales de autenticación en VoIP, que a menudo dependen de terceros o de arquitecturas centralizadas, lo que genera puntos de falla y problemas de privacidad. El artículo presenta un modelo de autenticación basado en blockchain que no solo brinda seguridad, sino que también disminuye los costos de comunicación. El modelo muestra un rendimiento superior y ha sido verificado con la herramienta AVISPA, corroborando su robustez contra amenazas. Esta investigación proporciona un enfoque innovador para el desarrollo del estudio de factibilidad técnica de la tecnología blockchain en sistemas de telefonía IP, ya que ofrece perspectivas valiosas para mejorar la autenticación en comunicaciones VoIP.

En 2022, en Human-Centric Computing and Information Sciences, el artículo titulado "Mecanismo de Autenticación Basado en Blockchain Ligero y Escalable para Comunicación Segura por VoIP", escrito por A. El Azzaoui, M. Y. Choi, C. H. Lee y J. H. Park, aborda las preocupaciones sobre seguridad y privacidad en las diferentes aplicaciones usadas durante la pandemia de COVID-19 para las reuniones virtuales. La investigación presenta una solución innovadora para la autenticación en videoconferencias mediante blockchain. Los autores proponen un mecanismo que utiliza un algoritmo de consenso basado en tiempo para mejorar la escalabilidad y reducir la latencia. Esta investigación es relevante para la

tesis sobre la implementación de blockchain en sistemas de telefonía IP, ya que proporciona un modelo que optimiza la privacidad y la autenticación. Sus resultados sobre la baja latencia pueden ofrecer una referencia valiosa.

En 2024, en Journal of Scientific and Engineering Research (JSAER), se publicó el artículo titulado "Asegurar el proceso de registro de usuarios en un sistema de telefonía IP utilizando tecnologías blockchain y KYC", escrito por S. J. N. P. Sonon, T. Djara, A. W. Bello y M. Ousmane. Este estudio se centra en desplegar una solución robusta para proteger las redes de telefonía IP mediante el uso de la tecnología blockchain con técnicas de KYC, reconocimiento facial y OTP (contraseña de un solo uso). En el artículo, los autores realizaron una comparación entre dos tipos de cadena de bloques, Ethereum e Hyperledger Fabric, siendo esta última la seleccionada, ya que cuenta con una variedad de lenguajes de programación para los contratos inteligentes. En la investigación se destacó cómo Hyperledger Fabric brinda una solución más adecuada para garantizar la confidencialidad y seguridad de los datos en el contexto de las redes de comunicación. Este estudio es relevante para nuestra investigación, pues ofrece un análisis detallado de los criterios utilizados para seleccionar la tecnología blockchain más adecuada para el caso de estudio a realizar.

En 2024, en la Escuela Politécnica Nacional (EPN) de Quito, se llevó a cabo la tesis de grado titulada "Estudio de las tecnologías Blockchain y sus aplicaciones en redes celulares 5G, 6G y en seguridades: estudio de la tecnología Blockchain y sus aplicaciones en redes 5G Y 6G", escrita por W. A. Espinosa Quimbita. Esta tesis indaga a fondo la tecnología blockchain, abordando algoritmos de consenso, funcionamiento y estructura. También se examina cómo blockchain se integra con las redes de nueva generación (5G y 6G), recalcando aplicaciones de la tecnología en la industria de las telecomunicaciones. El análisis desarrollado se centra en los beneficios ofrecidos por blockchain, tales como la transparencia e inmutabilidad, y al final se presentan las ventajas del impacto de esta tecnología en las redes avanzadas. Este trabajo de grado aporta una visión integral de cómo blockchain puede optimizar la transparencia y eficiencia en redes avanzadas. El entendimiento de las aplicaciones en las redes 5G y 6G brinda útiles perspectivas para aplicar estos conceptos en la telefonía IP, permitiendo la adaptación de blockchain para aumentar el rendimiento y la seguridad en sistemas de comunicación

4. Justificación:

La telefonía es un mecanismo universal de comunicación, en la era digital actual, la voz se puede transportar a través del protocolo IP, lo que representa una solución para ahorrar costos y flexibilizar la comunicación. No obstante, la seguridad y la privacidad de las comunicaciones son aspectos fundamentales para cualquier individuo o empresa. Sin embargo, la telefonía IP, siendo un sistema de comunicación en constante crecimiento, presenta vulnerabilidades que ponen en riesgo estos pilares fundamentales. Las redes de telefonía IP tradicionales carecen de mecanismos robustos de seguridad y cifrado, lo que las hace susceptibles a ataques como la interceptación de llamadas, el espionaje y el robo de datos. Esta situación genera un panorama preocupante, especialmente en el ámbito empresarial y gubernamental, donde la confidencialidad de la información es crucial.

La implementación de tecnología blockchain en la telefonía IP tiene el potencial de transformar radicalmente la seguridad y la privacidad de las comunicaciones. Blockchain, con su naturaleza descentralizada, inmutable y transparente, puede brindar un entorno seguro y confiable para las comunicaciones telefónicas.

Steck & Garrido (2021) afirman que la tecnología blockchain trae un beneficio adicional o más bien un obsequio de gran valor, pues indican que su diseño es inmune a lo que es común hoy en día, los ataques exteriores. Este obsequio se conoce como Security by Design que en español se traduce como «Seguridad por diseño». Esta filosofía lo que busca es que los controles de seguridad se incorporen desde las etapas iniciales del diseño de un producto y la implementación de la tecnología blockchain puede adaptar este principio asegurando que la seguridad este incluida desde el inicio. (p. 52).

Este proyecto de grado se alinea perfectamente con la línea de investigación protocolos de transmisión y recepción del grupo de investigación "GNET" de las UTS. El estudio de factibilidad técnica de la tecnología blockchain en la telefonía IP contribuirá al fortalecimiento de estas líneas de investigación, generando conocimiento y aportando soluciones innovadoras a un problema de gran relevancia actual. Este proyecto de grado representa un aporte significativo al campo de conocimiento en el área de seguridad informática y comunicaciones. La investigación y el análisis de la viabilidad de la tecnología blockchain en la telefonía IP abrirá nuevas posibilidades para el desarrollo de sistemas de comunicación más seguros, privados y eficientes.

5. Marcos referenciales:

Marco teórico

En el presente marco teórico se abordarán los fundamentos esenciales para el desarrollo de esta investigación, los cuales se centran en tres teorías principales: la teoría de sistemas distribuidos, la teoría de la telefonía IP y la teoría de la tecnología blockchain. Estas áreas conceptuales son clave para comprender las características, beneficios y desafíos de la integración de blockchain en redes de telefonía IP, lo que permitirá asegurar una infraestructura más eficiente, segura

y escalable. A partir de estas teorías, se explorarán sus principios y cómo interactúan en un entorno convergente de telecomunicaciones avanzadas.

Teoría de las Redes Distribuidas

Los sistemas información han venido creciendo a lo largo de los años gracias los avances de la computación y las telecomunicaciones. Esta última que se encarga de conectar grandes volúmenes de usuarios a través del envío de voz, datos y video por medio de redes de comunicación ya sean LAN, MAN o WAN. Todo esto ha permitidos que aparezcan centros de cómputo donde se desarrollan diferentes aplicaciones para realizar procesamiento distribuido de tareas.

Jiménez et al. (2017) define un sistema distribuido como un “conjunto de computadores autónomos interconectados”. (p. 1). Para ahondar en esta definición es importante saber que, si dos computadores son capaces de enviarse información entre ellos, se les considera que están interconectados. Y esta conexión puede ser a través de cualquier medio de transmisión, ya sea alámbrico (cobre o fibra óptica) o inalámbricos (enlaces microondas, enlaces satelitales).

Características del diseño de sistemas distribuidos:

- **Transparencia:** un sistema distribuido se considera transparente si este oculta al usuario la forma en la que funciona o fue creado. Es decir, el usuario tiene la percepción de que en un solo aparato local trabaja el sistema. Esta característica debe permitir que el usuario no sepa donde se alojan los datos.
- **Escalabilidad del sistema:** el usuario no sabe cuándo se incorpora una nueva máquina al sistema.
- **Flexibilidad :** se permite modificar el diseño inicial del sistema.
- **Confiabilidad:** una computadora puede reemplazar a otra en caso de que se presente un fallo para continuar con la labor asignada.
- **Desempeño:** esta característica se refiere a como el sistema responde a las peticiones de los usuarios, aquí juega un papel importante el tiempo de respuesta, donde se incluyen varios factores tales como latencia de red, carga de trabajo y balanceo, disponibilidad y fallas.
- **Funcionalidad :** esta característica se refiere a que el sistema distribuido cumpla la función para la cual fue diseñado de forma eficiente, facilitando el trabajo.
- **Seguridad:** un sistema distribuido debe contar con mecanismos de seguridad que permitan mitigar factores de riesgo y que a su vez ayuden a proteger la información.

Los sistemas distribuidos tienen diferentes tipos de arquitectura, la primera es la cliente-servidor donde una computadora cumple con el papel de servidor y puede realizar diferentes tareas o servicios y el cliente es la computadora o usuario final que solicita dicho servicio. La segunda arquitectura es la de igual a igual (peer-to-peer) donde no existe ninguna máquina que trabaje como servidor central. Aquí todos los nodos son tanto clientes como servidores, por tanto, ninguna computadora está destinada a servir al resto. Por último, la arquitectura basada en componentes, donde su enfoque es crear componentes que puedan ser reutilizables e independientes, es decir, se distribuye la funcionalidad del sistema en estos componentes para facilitar la gestión del sistema.

Teoría de la Telefonía Sobre IP

La telefonía IP se definirá como la serie de servicios y protocolos asociados con el transporte de comunicación de voz por internet, independientemente de los dispositivos del punto extremo. En los años noventa el protocolo de internet (IP) se expandía, esto abrió la posibilidad de transmitir el servicio de voz y otro tipo de comunicaciones multimedia a través de las redes de datos, representando una evolución natural de las telecomunicaciones. Dicha evolución trajo consigo beneficios como una forma de comunicación más flexible y económica, rompiendo barreras de las redes telefónicas conmutadas.

Tres décadas después, la telefonía IP ha experimentado cambios considerables desde su surgimiento, pues la estandarización de protocolos como el SIP (Protocolo de inicio de sesión) y RTP (Protocolo de transporte en tiempo real) han ayudado a que a nivel global se adopte la tecnología.

Valiente Hernández (2024) en su trabajo de fin de grado llamado Despliegues de Telefonía IP. Validación en diferentes entornos, menciona una serie de ventajas de la telefonía IP sobre la telefonía analógica:

En la telefonía IP se suprime el uso de infraestructuras dedicadas solo para el servicio de voz, ya que al trabajar sobre el protocolo IP se permite utilizar las redes existentes. En cambio, en la telefonía analógica se debe tener una infraestructura solo para este servicio.

La segunda ventaja que menciona Valiente Hernández se puede resumir en la palabra “movilidad”, pues la telefonía IP permite realizar y recibir llamadas desde cualquier lugar con acceso a internet, a diferencia de la telefonía analógica, que se limita a una ubicación física.

Es importante mencionar que la telefonía IP cuenta con una característica que la pone por encima de la telefonía analógica, pues es altamente escalable porque es más económica. (p. 9)

Protocolo de transporte en tiempo real (RTP)

Protocolo de transmisión en tiempo real, proporciona marcas de tiempo, números de series y otros métodos para garantizar el tiempo de procesamiento durante la transmisión de datos en tiempo real. Este protocolo se desarrolló como una guía para gestionar el transporte de tráfico multimedia en tiempo real. Normalmente, opera sobre el Protocolo de Datagramas de Usuario (UDP) en la capa de transporte del modelo OSI, ya que permite cumplir con las estrictas demandas de tiempo que exige el tráfico en tiempo real, aunque ello implique sacrificar la fiabilidad en la entrega de los paquetes (Vinueza Beltrán, 2015, p. 31).

Protocolo de control en tiempo real (RTCP)

Un protocolo para asegurar la calidad del servicio y el control de los participantes. RTP y RTCP se usan juntos. El protocolo RTCP ofrece funciones para detectar la pérdida de paquetes y corregir errores, además de monitorear el flujo de datos de RTP proporcionando información sobre la calidad de la transmisión, incluyendo la pérdida de paquetes, la latencia (el tiempo que tarda un paquete desde que se envía hasta que llega al destino), y la congestión de la red. De igual manera, RTCP incluye mecanismos para corregir la pérdida de paquetes, como la retransmisión de aquellos que se han perdido y el ajuste dinámico de la velocidad de bits para reducir dicha pérdida (Arce, 2024, p.74).

Protocolo de inicio de sesión (SIP)

SIP- RFC 3261, (Session Initiation Protocol o Protocolo de iniciación de sesión por sus siglas en inglés), es un protocolo de señalización utilizado para establecer una “sesión” entre dos o más participantes, modificar esa sesión y eventualmente terminar esa sesión. SIP es un protocolo de nivel de aplicación que no depende de las capas de transporte o de red, lo cual le permite operar tanto sobre TCP como sobre UDP. Sin embargo, es frecuente que las implementaciones usen SIP sobre UDP debido a su simplicidad y mayor rapidez en comparación con TCP (Del Valle Torres, 2012, p.2).

Estándar H.323

H.323 es la tecnología básica para la transmisión de audio, vídeo y datos en tiempo real por redes basadas en paquetes IP. La Versión 1 de la norma fue propuesta por la Comisión de Estudio 16 del UIT-T y aceptada en octubre de 1996 (La Versión 1 No garantiza la QoS). La norma actual es la Versión 8 de H.323 aprobada en noviembre de 2022. H.323 define cuatro componentes principales para un sistema de comunicaciones basado en red:

- Terminales: equipos de los usuarios finales, se encargan de codificar y decodificar la información multimedia.
- Pasarelas: Gateway con interfaces para interconectar diferentes tipos tecnologías, son intermediarios.
- Guardianes de puerta: brindan servicios a los terminales de usuarios como control de llamadas y controlan el acceso a la red.
- Unidades de control multipunto MCU: proporciona capacidad para que los usuarios y pasarelas participen en conferencia. También asocian varias sesiones y mezclan los flujos de audio y video.

Asterisk

Asterisk es una plataforma de código abierto (GNU) para establecer centrales de comunicaciones IP PBX, enlaces VoIP, servidores de conferencias, etc. Está diseñado para correr en Linux y es utilizado por pequeñas, medianas y grandes empresas en todo el mundo, pues tiene una gran variedad funcionalidades como: cola de espera, transferencia de llamadas, captura de llamadas, desvío de llamadas, música en espera, identificación de llamadas, buzón de voz, grupo de llamada, mensaje de bienvenida, entre otros y ventajas tales como:

- Es de fácil instalación y configuración, pues se implementa por software.
- Es de fácil administración porque cuenta con una interfaz intuitiva y simple.
- No requiere de un cableado especial.
- Es escalable, lo que permite ir agregando extensiones (usuarios – teléfonos) para ir expandiendo la red.
- Cuenta con funcionalidades que permiten canalizar llamadas y enrutarlas, mejorando la productividad.
- Interactúa con la telefonía tradicional mediante interfaces analógicas tales como FXO que es el puerto que recibe el servicio de línea telefónica y FXS que es el puerto que proporciona el servicio de la línea telefónica.

Marco conceptual

El marco conceptual de este proyecto de investigación aborda los conceptos fundamentales necesarios para entender el funcionamiento y aplicaciones de la tecnología blockchain y sus componentes. Se analizará el concepto de redes Peer to Peer (P2P), que permiten la interacción directa entre nodos; los contratos inteligentes, que automatizan acuerdos sin intermediarios; y los algoritmos de consenso, esenciales para la validación de transacciones.

P2P

Los sistemas P2P permiten compartir cualquier archivo sin ningún intermediario. Es una de las redes más antiguas que prácticamente surgió después de la creación de los ordenadores personales. Las redes peer-to-peer se conocen como red entre pares o red de igual a igual. Consiste en un modelo de comunicación descentralizado, es decir, no se requiere un servidor central, sino que cada parte o usuario actúa como igual y tiene la función de servidor o cliente. Una ventaja adicional es que cada usuario puede administrar su propio dispositivo.

Contratos inteligentes

El concepto de Smart Contract apareció en el año 1994, por iniciativa del experto computacional Nick Szabo, quien quería crear protocolos de transacciones electrónicas que ejecutaran correctamente los términos de un contrato o acuerdo. El propósito de este tipo de protocolo es eliminar la necesidad de tener un intermediario para negociar, administrar y respaldar el contrato entre dos partes (Ramírez, 2020).

Un contrato inteligente es en realidad un programa informático que se ejecuta dentro de una blockchain. Incluye tanto código como datos y nunca es controlado por un usuario, si no que siempre opera de acuerdo con su programación. Es por eso que un protocolo de este tipo puede administrar las transacciones por sí mismo de manera infalible, y no requiere la presencia de un tercero en la relación entre los dos contratistas. Cualquier contrato inteligente tiene programado en el código una secuencia de condiciones que deben cumplirse para que se validen las operaciones y transacciones en la Blockchain. Una vez confirmadas las condiciones específicas, estando estos datos disponibles en blockchain, el contrato inteligente ejecuta un protocolo basado en declaraciones condicionales de tipo if/then para que ambas partes involucradas reciban lo establecido para completar el contrato.

Algoritmo de consenso

La expresión "algoritmo de consenso" se puede analizar descomponiéndola en sus dos partes, Algoritmo como "un grupo limitado de instrucciones o normas establecidas y organizadas que facilitan la ejecución de una tarea determinada o la resolución de un problema". En este contexto, hace referencia a un procedimiento informático que realiza una serie de etapas para obtener un resultado y consenso hace referencia "al acuerdo entre diversas partes". En el contexto de la cadena de bloques, el consenso conlleva que diversos nodos (participantes) de la red alcancen un pacto sobre el estado de los datos, asegurando que todos tengan la misma copia de los datos. Así pues, el término "algoritmo de consenso" alude a un grupo de normas o procedimientos que facilitan a los distintos nodos de una red blockchain alcanzar un consenso común en cuanto a la validez y el estado de las transacciones.

Protocolos de consenso

También conocidos como mecanismos de consenso, estos protocolos son algoritmos que le permiten a los sistemas distribuidos crear entornos de trabajo seguros. Estos mecanismos se responsabilizan de la aprobación de todos los nodos que hacen parte de la red blockchain sobre la información que hay en ella. En un entorno más práctico, estos mecanismos ayudan a que los nodos reconozcan que el último bloque fue agregado a la cadena de forma correcta, sin errores y sin alteración (Díaz et al., 2022). Algunos de los mecanismos más usados por el momento son prueba de trabajo, autoridad y participación.

6. Objetivo general y objetivos específicos:

Realizar un estudio de factibilidad técnica en sistemas de telefonía IP utilizando tecnología blockchain para mejorar la seguridad, privacidad y eficiencia de las comunicaciones telefónicas

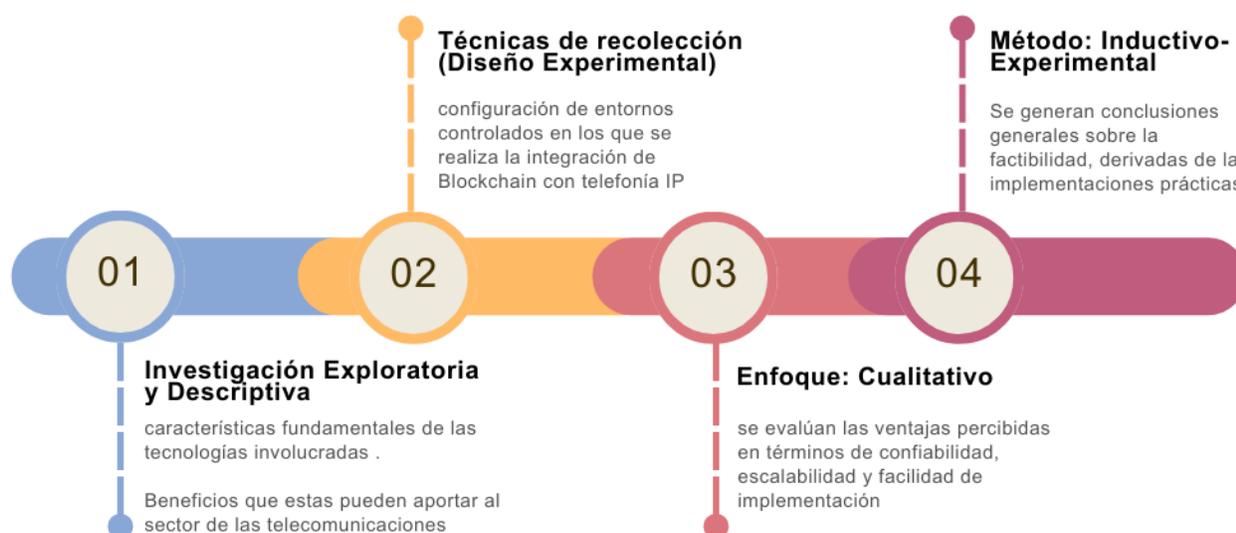
- Explicar los principios básicos y las características esenciales de la tecnología blockchain para proporcionar una comprensión fundamental que sirva de base para su aplicación en la telefonía IP.
- Identificar los beneficios potenciales que la tecnología blockchain puede aportar al sector de las telecomunicaciones, enfocándose en aspectos como seguridad, privacidad, eficiencia y transparencia de las operaciones de comunicación.
- Desarrollar un prototipo o simulación que integre una red telefónica con una planta Grandstream, contratos inteligentes en plataforma Blockchain, y una API, para validar la funcionalidad y efectividad de la tecnología blockchain en un entorno controlado.
- Proporcionar recomendaciones y pautas para la implementación exitosa de la tecnología blockchain en sistemas de telefonía IP, basadas en los hallazgos del estudio, para guiar a las organizaciones en la adopción de esta tecnología y mejorar la seguridad y eficiencia de sus comunicaciones

7. Metodología:

El presente estudio se clasifica como una investigación de tipo exploratoria y descriptiva. Es exploratoria porque busca analizar la viabilidad técnica de integrar la tecnología blockchain con sistemas de telefonía IP, un tema que aún no ha sido ampliamente documentado en el ámbito técnico. Asimismo, es descriptiva ya que detalla las características fundamentales de las tecnologías involucradas y los beneficios que estas pueden aportar al sector de las telecomunicaciones, particularmente en aspectos como seguridad, privacidad, eficiencia y transparencia.

El enfoque de esta investigación es de tipo cualitativa, se evalúan las ventajas percibidas en términos de confiabilidad, escalabilidad y facilidad de implementación, mediante un análisis de los entornos experimentales. El método utilizado es inductivo-experimental, ya que parte de la observación de fenómenos específicos derivados de las implementaciones prácticas para generar conclusiones generales sobre la factibilidad y los beneficios de la integración de blockchain en sistemas de telefonía IP. Este método permite construir un marco técnico robusto basado en evidencia experimental.

Para la recolección de datos, se emplean técnicas de diseño experimental, que incluyen la configuración de dos entornos controlados en los que se realiza la integración de blockchain con telefonía IP. El primer entorno utiliza un servidor Issabel virtualizado, al cual se le desarrolló una API basada en la interfaz Asterisk REST Interface (ARI) para extraer información detallada de las llamadas y registrar dichos datos en una blockchain privada utilizando Multichain. El segundo entorno se basa en la integración de una planta telefónica Grandstream UCM6300A, en la cual se implementó una API AMI para capturar y transmitir información de las llamadas hacia la misma blockchain.



8. Avances realizados:

No aplica.

9. Resultados esperados:

1. Informe detallado sobre los principios y características fundamentales de la tecnología blockchain, incluyendo su estructura, funcionamiento y posibles aplicaciones.
2. Informe sobre el potencial beneficio de la tecnología blockchain en el sector de las telecomunicaciones con un enfoque en la seguridad, la privacidad, la eficiencia y la transparencia de las operaciones de comunicación.
3. Desarrollo de un prototipo o simulación que integre una red telefónica con una planta Grandstream, contratos inteligentes y una API, demostrando la viabilidad de la propuesta. Además, se entregarán los resultados de las pruebas y la evaluación del prototipo en un entorno controlado.
4. Artículo que presente los hallazgos del estudio de factibilidad técnica y sugiere estrategias para la implementación de la tecnología blockchain en sistemas de telefonía IP.

10. Cronograma:

Actividad (Semanal)	Fase 1				Fase 2				Fase 3					Fase 4				Fase 5				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Revisar literatura científica y técnica sobre los principios y fundamentos de la tecnología blockchain.	█	█																				
Elaborar un documento que describa los componentes y funcionamiento de blockchain.			█																			
Crear diagramas y esquemas visuales que ilustren el proceso de blockchain.				█																		
Recopilar y analizar estudios de caso donde blockchain se haya implementado en telecomunicaciones.					█	█																
Analizar informes y documentos técnicos que aborden los posibles beneficios de la integración de blockchain en sistemas de telecomunicaciones.							█	█														
Redactar un informe que resuma los beneficios identificados y su relevancia para el sector de las telecomunicaciones.									█	█												
Preparar la planta telefónica Grandstream para la simulación, incluyendo la configuración inicial, la interconexión de los dispositivos y la verificación de que todos los componentes de la red de telefonía IP funcionan correctamente											█	█										
Diseñar, codificar y desplegar los contratos inteligentes alguna plataforma blockchain,												█										
Configurar y conectar la API que permitirá la integración de la planta telefónica Grandstream con la red blockchain, garantizando una comunicación efectiva y segura entre ambos sistemas.												█	█									
Ejecutar una serie de pruebas controladas para validar la funcionalidad del sistema, documentando los resultados y realizando ajustes necesarios para asegurar que el sistema cumple con los objetivos planteados.															█							
Evaluar el rendimiento del sistema integrado en términos																█	█					

11. Bibliografía:

Guerrón Subía, L. I. (2021). Modelo de seguridad sobre la telefonía IP/OPEN Ssource en base a la metodología PTES en la empresa Sinfotecnia (Bachelor's thesis).

Almonte, M. (2019). Blockchain y propiedad intelectual: investigación sobre sus avances y posibles usos. Anuario Dominicano de Propiedad Intelectual.

Steck, C., & Garrido, E. F. (2021). Telecomunicaciones: de la revolución de datos a la revolución blockchain. In Blockchain: la revolución industrial de internet (pp. 50-56). Gestión 2000.

Carrizo Saavedra, A. F. (2021). Ventajas competitivas del uso de Tecnología Blockchain en el sector Telecomunicaciones de Argentina para el período 2021-2025 (Master's thesis).

Rodríguez Espinoza, E. A. (2020). Estudio de la tecnología Blockchain para el aseguramiento de los dispositivos IOT (Bachelor's thesis, Quito: Universidad de las Américas, 2020).

Carrión Basantes, A. K. (2018). Análisis de la utilización de la Tecnología Blockchain para la gestión de la información en Sistemas de Alarmas Residenciales (Bachelor's thesis, Quito, 2018.).

Briceño Gómez Sánchez, R. J. (2020). Análisis del servicio telefonía VOIP siguiendo los estándares de seguridad informática. Una revisión de la literatura científica.

Cavagna, M. C. (2022). Análisis de factibilidad del uso de la tecnología blockchain para la trazabilidad de medicamentos en Argentina.

Sonon, S. J. N. P., Djara, T., BELLO, A. W., & OUSMANE, M. (2024). Securing the User Registration Process in an IP Telephony System Using Blockchain and KYC Technologies. Journal of Scientific and Engineering Research (JSAER), 11(1), 238-247.

Kara, M., Aydin, M. A., & Balık, H. H. (2022). Bcvop2p: Decentralized Blockchain-Based Authentication Scheme for Secure Voice Communication. Intelligent Automation & Soft Computing, 31(3).

El Azzaoui, A., Choi, M. Y., Lee, C. H., & Park, J. H. (2022). Scalable lightweight blockchain-based authentication mechanism for secure VoIP communication. Hum.-Cent. Comput. Inf. Sci, 12(8).

Espinosa Quimbita, W. A. (2024). Estudio de las tecnologías Blockchain y sus aplicaciones en redes celulares 5G, 6G y en seguridades: estudio de la tecnología Blockchain y sus aplicaciones en redes 5G Y 6G (Bachelor's thesis, Quito: EPN, 2024.).

* Organización para la Cooperación y Desarrollo Económico (OCDE)

** PA: Proyecto de Aula, PI: Proyecto integrador, TI: Trabajo de Investigación, RE: Recursos Educativos Digitales Abiertos (REDA)