Viabilidad del diseño e implementación de una aplicación de mensajería instantánea de voz basada en Blockchain

Eduardo Luis Ojeda

Álvaro Suarez Sarmiento

Grado de Ingeniería en Tecnologías de la Telecomunicación

ULPGC Universidad de Las Palmas de Gran Canaria

ETSE ESCUELA DE INGENIERÍA DE TELECOMUNICACIÓN Y ELECTRÓNICA

INTRODUCCIÓN

En un mundo digital cada vez más interconectado, la seguridad y privacidad en las comunicaciones son esenciales. Este Trabajo Fin de Grado evalúa la viabilidad de una aplicación de mensajería instantánea centrada en la seguridad, utilizando tecnologías avanzadas como Blockchain o Nostr para garantizar seguridad de extremo a extremo y resistencia a la censura. La aplicación permite a los usuarios controlar sus datos mediante cifrado avanzado. El estudio concluye evaluando la adaptación, escalabilidad, facilidad de uso e integridad de las comunicaciones, buscando ofrecer una herramienta de mensajería segura, eficiente y flexible.

OBJETIVOS

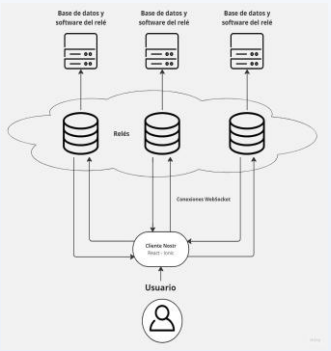
O1. Conocer y comprender profundamente el funcionamiento de Blockchain: su arquitectura, así como protocolos, plataformas y tecnologías asociadas.

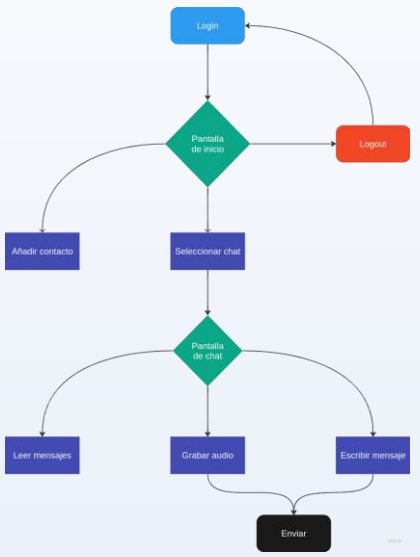
O2. Estudiar en profundidad la implementación de redes aplicaciones de mensajería instantánea de voz basadas en Blockchain o similares (*Nostr*) a través del uso de los diferentes protocolos, plataformas y tecnologías que se encuentren disponibles para ello.

O3. Estudio de la viabilidad del diseño e implementación de la aplicación de mensajería instantánea de voz y potencial implementación haciendo uso de los protocolos, plataformas y tecnologías más adecuadas como es el caso de *Nostr*.

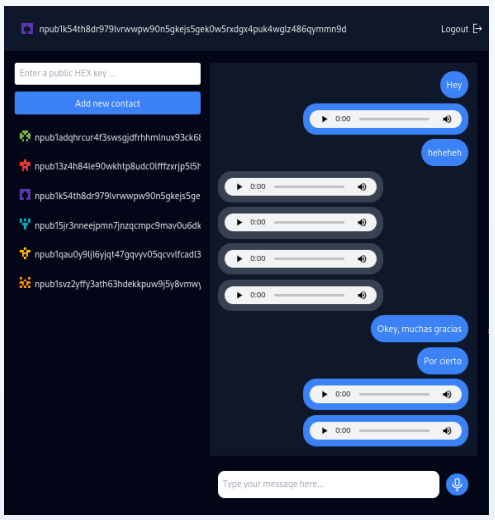
METODOLOGÍA

La metodología llevada a cabo para el desarrollo de este TFG ha consistido en dos etapas. La primera, el análisis de la viabilidad de tecnologías descentralizadas, donde se estudió en profundidad la tecnología Blockchain (la blockchain de Solana en particular) y el protocolo Nostr [1]. La segunda etapa consistió en el desarrollo y estudio de la aplicación, donde se analizó tanto el sistema de comunicación y conexión con las diferentes partes del sistema, como la interfaz para brindar una buena experiencia de usuario.

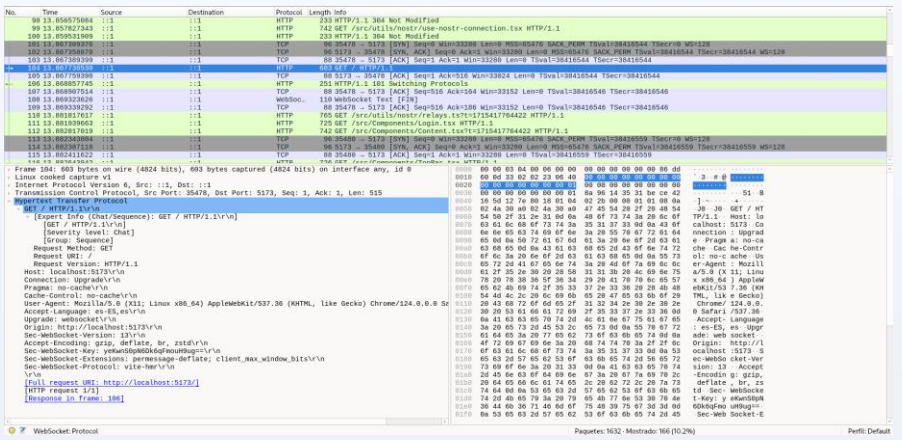




RESULTADOS



Los resultados obtenidos se pueden visualizar de manera sencilla viendo la interfaz de usuario desarrollada y observando el tráfico capturado con Wireshark. Con el análisis del tráfico podemos ver los protocolos de encriptación utilizados y el funcionamiento de todo el sistema implementado.



CONCLUSIONES

- La aplicación de mensajería instantánea desarrollada sobre el protocolo Nostr funciona correctamente y cumple con los requisitos establecidos.
- El uso de Websockets ha facilitado el entendimiento de las conexiones bidireccionales sobre TCP, crucial para la mensajería instantánea.
- El estudio de Blockchain y Nostr ha brindado un conocimiento profundo sobre la seguridad e identidad de los usuarios en la red.
- La investigación previa ha sido esencial para superar problemas y desarrollar habilidades de ingenio y adaptación.
- El sistema integrado permite la creación de nuevas conversaciones, envío y recepción de mensajes, y un sistema de autenticación eficaz.

REFERENCIAS

[1] Nostr. (2023, julio). The Protocol. En línea. Disponible en: https://nostr.how/es/the-protocol (accedido por última vez el 25 de marzo de 2024).