NQX — Hoja de Ruta Pública

Introducción

El sistema NQX fue creado para permitir comunicación gratuita, intercambio de mensajes y datos sin intermediarios ni servidores centralizados. Está diseñado con prioridad absoluta en la privacidad y la ausencia total de recopilación de datos. Su funcionalidad está disponible en cualquier parte del mundo, sin importar el país, la condición social o la ubicación del usuario.

Definiciones

— Usuario: participante de la red NQX, sin registro obligatorio ni entrega de datos personales.
— Comunicación directa: intercambio de datos entre dispositivos sin intervención de terceros ni nodos centralizados.
— Criptoinmersión profunda: término propio de NQX que describe un conjunto de métodos criptográficos que protegen tanto el contenido como la existencia misma de la comunicación.
— Sesión: período temporal de interacción cuyos datos no se guardan una vez finalizado.

Disposiciones

— No se almacena información: mensajes, archivos ni metadatos.
— Autonomía: funcionamiento sin registro obligatorio y con posibilidad de anonimato total.
— Comunicación grupal resistente ante caídas o desconexiones de Internet.
— Invisibilidad de las comunicaciones: el tráfico no puede ser interceptado, censurado ni atribuido a participantes.
— Los métodos criptográficos usados constituyen la base de la criptoinmersión profunda.
— Gratuito: acceso sin restricciones financieras ni suscripciones.

Objetivos

1. Garantizar comunicación segura y estable incluso en condiciones extremas.
2. Construir una infraestructura independiente resistente a bloqueos y censura.
3. Asegurar el anonimato y la privacidad de cada participante.
4. Proveer medios de comunicación universales accesibles desde cualquier lugar del mundo.
5. Mantener facilidad de uso sin necesidad de hardware adicional.

Modelo de amenazas

El sistema se diseñó considerando las siguientes amenazas:
— Censura local y global.
— Acumulación y análisis deliberado de datos personales por servicios globales.
— Análisis de interacciones que permiten construir mapas de relaciones y hábitos de los usuarios.
— Intentos de bloquear los canales de comunicación.
— Cortes de Internet tanto locales como globales.

Fases de implementación

Fase 1 — Funcionalidad fundamental
— Comunicación directa entre usuarios sin intervención de terceros ni nodos centrales.
— Total autonomía sin registro.
— Acceso gratuito desde cualquier parte del mundo.
— Soporte para mensajes, archivos, audio y video.
— Llamadas de voz P2P sin SIM ni número telefónico.
— Intercambio seguro e instantáneo de claves.
— Criptoinmersión profunda para invisibilidad y protección contra interceptación.

Fase 2 — Expansión de capacidades
— Creación y disolución dinámica de grupos protegidos sin almacenamiento tras la sesión.
— Arquitectura modular con componentes intercambiables.
— Integración de canales multiprotocolo.
— Herramientas avanzadas para compartir archivos y multimedia.

— Videoconferencias protegidas.

Fase 3 — Fortalecimiento y adaptación
— Resiliencia frente a nuevas amenazas técnicas y de censura.
— Actualización de métodos criptográficos y criptoinmersión.
— Anticipación de riesgos tecnológicos y de red.

Fase 4 — Ecosistema e integraciones
— API para integrar NQX con servicios externos.
— Soporte de pagos anónimos y microtransacciones.
— Integración con llaves de hardware y dispositivos seguros.
— (Sin almacenamiento: integraciones no alteran la política de no guardar datos ni metadatos).

Fase 5 — Comunidad y autogestión
— Sistema descentralizado de gobernanza del proyecto (DAO).
— Mecanismos transparentes de propuestas y votaciones.
— Programas de becas para desarrolladores e investigadores.
— Pruebas públicas y recompensas por vulnerabilidades encontradas.

Conclusión

Avanzamos hacia un sistema de comunicación independiente, resistente y globalmente accesible que mantiene la libertad incluso frente a bloqueos, vigilancia y represión. NQX no es solo una herramienta, es un espacio donde cada persona sigue siendo libre y su comunicación es invisible y protegida frente a quienes intentan controlarla.