NOX – خارطة الطريق

مقدمة

تم إنشاء نظام NOX من أجل التواصل المجاني وتبادل الرسائل والبيانات بدون وسطاء أو خوادم مركزية. تم تطوير النظام مع أولوية للخصوصية ورفض جمع البيانات بشكل مبدئي. الوظائف متاحة في أي مكان في العالم بغض النظر عن الدولة أو الوضع الاجتماعي أو موقع المستخدم.

التعاريف

– المستخدم: هو مشارك في شبكة NOX لا يخضع لتسجيل إلزامي ولا يقدم بيانات شخصية.

– الاتصال المباشر: تبادل البيانات بين الأجهزة بدون طرف ثالث أو عقد مركزية.

– التشفير العميق: مصطلح خاص بنظام NOX يشير إلى مجموعة من الأساليب التشفيرية التي تضمن ليس فقط حماية المحتوى، بل أيضاً إخفاء وجود الاتصال نفسه.

– الجلسة: فترة زمنية مؤقتة من التفاعل، لا يتم فيها حفظ البيانات بعد الانتهاء.

المبادئ

– لا يتم تخزين البيانات: المحادثات والملفات والبيانات الوصفية لا يتم حفظها في النظام.

– الاستقلالية: العمل بدون تسجيل إلزامي مع إمكانية إخفاء الهوية بالكامل.

– مرونة الاتصال الجماعي عند انقطاع أو فقدان الاتصال بالإنترنت.

– خفاء الاتصال: لا يمكن اعتراض أو رقابة أو تحديد هوية المشاركين.

– الأساليب التشفيرية المستخدمة تشكل أساس آلية التشفير العميق.

– مجاني: الوصول بدون قيود مالية أو اشتراكات.

الأهداف

1. ضمان اتصال آمن ومستقر في جميع الظروف، بما في ذلك الظروف القصوى.

2. بناء بنية تحتية مستقلة مقاومة للرقابة والحظر.

3. ضمان الخصوصية وإخفاء الهوية لكل مشارك.

4. توفير أدوات اتصال شاملة ومتاحة في أي مكان بالعالم.

5. الحفاظ على سهولة الاستخدام دون الحاجة إلى معدات إضافية.

نموذج التهديدات

– الرقابة المحلية والعالمية.

– جمع وتحليل البيانات الشخصية من قبل الخدمات العالمية.

– تحليل أنماط التفاعل لبناء خرائط العلاقات والعادات.

– محاولات حظر قنوات الاتصال.

– انقطاعات الإنترنت المحلية والعالمية.

مراحل التنفيذ

المرحلة 1 — الوظائف الأساسية

— اتصال مباشر بين المستخدمين بدون طرف ثالث أو عقد مركزية، مع دعم الاتصال الجماعي أثناء الانقطاع.

— التشغيل بشكل مستقل تمامًا بدون تسجيل.

— الوصول المجاني للوظائف من أي مكان.

— دعم الرسائل والملفات والصوت والفيديو.

— مكالمات صوتية P2P بدون شريحة SIM أو رقم هاتف.

— تبادل مفاتيح آمن وفوري.

— آلية التشفير العميق لحماية الاتصال وإخفائه.

المرحلة 2 — توسيع القدرات

— إنشاء وتفكيك المجموعات المحمية ديناميكياً بدون حفظ البيانات بعد انتهاء الجلسة.

— بنية معيارية لإضافة واستبدال المكونات بدون توقف النظام.

— دمج قنوات متعددة البروتوكولات لتحسين الموثوقية.

— أدوات موسعة لمشاركة الملفات والوسائط بأمان.

— مؤتمرات فيديو مشفرة.

المرحلة 3 — تعزيز الاستقرار والتكيّف

— تعزيز المقاومة ضد التهديدات التقنية والرقابية الجديدة.

– تحديث الأساليب التشفيرية وآليات التشفير العميق.

– الاستجابة الاستباقية للمخاطر التكنولوجية والشبكية المتغيرة.

المرحلة 4 – النظام البيئي والتكاملات

– واجهة برمجة تطبيقات (API) لدمج NQX مع التطبيقات والخدمات الأخرى.

– دعم المدفوعات المجهولة والمعاملات الصغيرة داخل الشبكة.

– التكامل مع مفاتيح التشفير والأجهزة الآمنة.

– (بدون تخزين البيانات: التكاملات لا تغير المبدأ الأساسي بعدم حفظ المحتوى أو البيانات الوصفية).

المرحلة 5 – المجتمع والإدارة الذاتية

– إنشاء نظام لامركزي للإدارة الجماعية للمشروع (DAO).

– آليات شفافة للاقتراحات والتصويت على التغييرات.

– برامج منح للمطورين وباحثي الأمن.

– اختبارات مفتوحة ومكافآت للثغرات المكتشفة.

الخاتمة

نتجه نحو نظام اتصال مستقل، مرن، ومتاح عالميًا، يحمي حرية التواصل حتى تحت الضغط والحظر والاعتراض. NQX ليست مجرد أداة، بل فضاء يظل فيه كل فرد حرًا، حيث تكون التفاعلات محمية وغير مرئية لأولئك الذين يحاولون السيطرة عليها.