



NOX — Feuille de route

Introduction

Le système NOX est conçu pour la communication gratuite, l'échange de messages et de données sans intermédiaires ni serveurs centralisés. Il est développé avec une priorité absolue à la confidentialité et à l'absence de collecte de données. Ses fonctionnalités sont accessibles partout dans le monde, indépendamment du pays, du statut social ou de la localisation de l'utilisateur.

Définitions

- Utilisateur : participant du réseau NOX, sans inscription obligatoire ni fourniture de données personnelles.
- Communication directe : échange de données entre appareils sans tiers ni nœuds centralisés.
- Cryptage profond : terme propriétaire de NOX désignant un ensemble de méthodes cryptographiques assurant la protection du contenu et la dissimulation même de la communication.
- Session : période temporaire d'interaction, après laquelle les données ne sont pas conservées.

Dispositions

- Aucune conservation de données : les conversations, fichiers et métadonnées ne sont pas stockés.
- Autonomie : fonctionnement sans inscription obligatoire, avec anonymat complet possible.

- Résilience des communications de groupe en cas de perte de connexion Internet.
- Invisibilité des communications : le trafic ne peut pas être intercepté, censuré ou attribué à un utilisateur.
- Les primitives cryptographiques utilisées sont à la base du cryptage profond.
- Gratuité : accès sans frais ni abonnements.

Objectifs

1. Assurer une communication sûre et stable en toutes circonstances, même extrêmes.
2. Créer une infrastructure indépendante résistante à la censure et aux blocages.
3. Garantir l'anonymat et la confidentialité de chaque utilisateur.
4. Fournir des moyens de communication universels accessibles partout dans le monde.
5. Préserver la simplicité d'utilisation sans matériel supplémentaire.

Modèle de menace

Le système est conçu en tenant compte des menaces potentielles suivantes :

- Censure locale et globale.
- Collecte et analyse ciblées de données personnelles par les services mondiaux.
- Analyse des interactions pour cartographier les relations et habitudes.
- Tentatives de blocage des canaux de communication.
- Coupures Internet locales et globales.

Phases de mise en œuvre

Phase 1 — Fonctionnalité de base

- Communication directe entre utilisateurs sans tiers ni nœuds centralisés, résilience des groupes même sans Internet.
- Fonctionnement totalement autonome, sans inscription.
- Accès gratuit dans le monde entier, sans condition de pays ou de statut.
- Messagerie, échange de fichiers, appels audio et vidéo via canaux accessibles.
- Appels P2P sans carte SIM ni numéro.
- Échange de clés sécurisé et instantané.
- Cryptage profond assurant invisibilité et protection contre l'interception.

Phase 2 — Extension des capacités

- Création et dissolution dynamiques de groupes sécurisés, sans conservation de données.
- Architecture modulaire pour mise à jour sans interruption.
- Intégration multi-protocole pour fiabilité accrue.
- Outils avancés pour partage de fichiers et médias sécurisé.
- Vidéoconférences sécurisées.

Phase 3 — Renforcement et adaptation

- Résistance accrue face aux menaces techniques et de censure émergentes.
- Mise à jour des méthodes cryptographiques et du cryptage profond.
- Anticipation des risques technologiques et réseau.

Phase 4 — Écosystème et intégrations

- API pour intégrer NOX à d'autres applications et services.
- Prise en charge des paiements anonymes et microtransactions.
- Intégration avec clés et dispositifs matériels sécurisés.

— (Aucune conservation de données : intégrations sans modification du principe fondamental.)

Phase 5 — Communauté et gouvernance

- Système de gouvernance collective décentralisée (DAO).
- Mécanismes transparents de propositions et votes.
- Programmes de subventions pour développeurs et chercheurs en sécurité.
- Tests ouverts et récompenses pour vulnérabilités découvertes.

Conclusion

Nous avançons vers un système de communication global, résilient et libre, qui protège la liberté même sous censure ou surveillance. NOX n'est pas juste un outil — c'est un espace où la liberté individuelle est respectée et l'interaction reste protégée et invisible aux regards intrusifs.