



NOX — 路线图

引言

NOX 系统是为实现免费通信、消息和数据交换而设计的，无需中介和集中式服务器。该系统以隐私为优先原则，并坚持不收集数据。其功能可在全球任何地方使用，无论用户的国家、社会地位或地理位置如何。

定义

- 用户：NOX 网络的参与者，无需强制注册，也不提供个人数据。
- 直接通信：设备之间直接交换数据，无需第三方或集中节点参与。
- 深度加密：NOX 系统的专有术语，指一套加密方法，不仅保护内容，还隐藏通信行为本身。
- 会话：临时交互期，会话结束后数据不会被保存。

条款

- 不保存数据：对话、文件和元数据不会由系统保存。
- 自主性：无需注册即可使用，支持完全匿名。
- 即使在断网或失去连接的情况下，群组通信仍保持稳定。
- 通信隐身：通信流量无法被拦截、审查或识别参与者。
- 使用的加密方法（加密原语）是深度加密机制的基础。
- 免费访问：无财务限制或订阅费用。

目标

1. 在任何情况下，包括极端条件下，提供安全稳定的通信。
2. 构建一个抗审查和屏蔽的独立基础设施。
3. 确保每位参与者的匿名性和隐私。
4. 提供全球范围内可用的通用通信工具。
5. 保持使用简单，无需额外设备。

威胁模型

系统设计时已考虑以下潜在威胁：

- 本地和全球审查制度。
- 全球服务针对性收集与分析个人数据。
- 通过分析交互信息绘制用户关系和行为习惯图谱。
- 阻断通信通道的尝试。
- 本地和全球断网情况。

实施阶段

第一阶段 — 基础功能

- 用户间直接通信，无需第三方或中心节点，群组通信在断网时仍保持稳定。
- 完全自主运行，不需要注册。
- 全球免费访问功能，无地域、社会或位置限制。
- 支持消息、文件、音视频通信。
- 无需 SIM 卡或电话号码的 P2P 音频通话。
- 集成安全即时的密钥交换。
- 深度加密机制，确保通信隐身性和抗拦截性。

第二阶段 — 功能扩展

- 会话结束后自动解散的动态安全群组。
- 模块化架构，可动态添加/替换组件。
- 多协议通信渠道整合，提高可靠性。
- 增强型文件和媒体安全传输工具。
- 加密视频会议支持。

第三阶段 — 增强弹性与适应性

- 面对新技术与审查威胁时提高弹性。
- 更新加密方法与深度加密机制。
- 主动应对技术和网络风险变化。

第四阶段 — 生态系统与集成

- 提供 API 与第三方应用和服务集成。
- 支持网络内匿名支付和微交易。
- 集成硬件加密钥匙与安全设备。

—（不保存数据：集成不影响无存储原则）

第五阶段 — 社区与自治

- 建立去中心化的项目治理体系（DAO）。
- 提供提案与变更投票机制。
- 启动开发者与安全研究人员的资助计划。
- 公开测试与漏洞赏金机制。

结语

我们正在迈向一个独立、强韧且全球可用的通信系统，即使在审查、封锁或监听情况下，也能保持通信自由。NOX 不仅是工具，更是一个空间，让每个人都能自由沟通，其交互过程对试图控制的人来说不可见且受保护。