

ParaDigi 协议：点对点的社交网络

一个去中心化的信息自由世界


Liu Peng 2025.03.05

为什么我们需要新的社交网络？

- 中心化平台垄断用户关系
- 隐私泄露与数据滥用
- 政府监管与封锁风险

去中心化就够了吗？

- Mastodon：联邦架构的局限
- 区块链平台：代币成本的公平性问题
- 邀请制：限制用户多样性



如何在无第三方依赖下实现信任？

全序签名，重塑发布者身份

ParaDigi的答案

- 私钥签名消息序列
- 不可篡改的信任基石

消息：社交的原子单位

消息的力量

- 内容 + 互动 + 签名
- 时序关系定义真实性

一条消息说明不了什么

时序的意义

- 单独信息无意义
- 全序链表揭示行为模式

你无法隐藏你的过去

发布者的责任

- 分叉即恶意
- 完整性是信任的代价

谁能进入你的世界？

可见身份集合

- 基于互动的自定规则
- 信任的传递性

信任的边界

零成本身份的终结

对抗女巫攻击

- 新身份难以传播
- 互动决定可见性
- 节点过滤消息
- 互动放大优质内容

传播即奖励

激励的逻辑 & 惩罚的哲学

- 优质内容扩大影响力
- 垃圾信息自取灭亡

社交网络中的加密货币

- 高效共识机制
- 身份替代质押

隐私的悖论


公开透明下的隐私保护？

- 匿名公钥
- 系统外加密通信


欢迎，但不依赖

对第三方的态度

- 信息检索
- 广告平台
- 金融服务



世界本就没有中心



你的信息网络由谁定义？

前路漫漫

- 技术实现的复杂性
- 用户接受度的考验

ParaDigi: 从信任开始

liupeng@pdu.pub