

# 去中心化通讯

技术和挑战

李维

2019-12-29

# 去中心化可以解决这些问题吗？

- ◎ 垃圾：信息、电话
- ◎ 隐私
- ◎ 安全
- ◎ 权力：
  - 禁号
- ◎ 互通
- ◎ 网络的维护成本
  
- ◎ 现有体系可能重构吗？

# 通讯市场-分类

- ◎ 语音 | 数据
- ◎ 个人 | 企业
- ◎ 免费 | 收费
- ◎ 软件 | 硬件
- ◎ 应用：
  - > 呼叫中心
  - > 会议
  - > 直播

# 通讯市场-传统

- ◎ 基础电信： 6721亿元（2019年1-6月）
- ◎ 信息化和集成： OSS、MSS、BSS
- ◎ 设备： 华为、思科、中兴
- ◎ 历史：
  - > 电话网=》数据网
  - > 固网=》移动网
  - > 消失的巨头： 北电、朗讯.....
- ◎ 趋势：
  - > 运营商体系=》自主网？
  - > IP局限，IPFS启发：
    - ipv6或许只是一个过渡产品
  - > 隐私、权利保护

# 通讯市场-新兴

## ◎ 社交

- > WhatsApp
- > WeChat
- > Telegram

## ◎ 通信云

- > Twillio
- > 容联云通信
- > 个推
- > 极光推

# Players

- ◎ 电信运营商/设备运营商/通管局
- ◎ 社交网络：
- ◎ 商业机构：OS
- ◎ 非盈利机构：signal
- ◎ 区块链项目：社区

# 传统通讯技术

- ◎ Data
  - > IP、DNS、routing、switch
  - > 非IP的通讯技术
- ◎ Audio/Vedio
  - > H323
  - > SIP
  - > XMPP
  - > WEBRTC
- ◎ SMTP/IMAP/POP
- ◎ ICE: STUN/TURN
- ◎ Provisioning
- ◎ Billing

# 加密技术

- Public-key cryptography/asymmetric cryptography
  - > RSA/DSA/ECDSA/EDDSA
- PGP/GPG**
- Signal:
  - > XEdDSA/VXEdDSA
  - > X3DH
  - > Double Ratchet
  - > Sesame
- TOR: The Onion Router



# 去中心化通讯的技术

- P2P
- DID
- WIFI Direct、蓝牙、Lora
  - > **IOS: MultipeerConnectivity**
  - > Android:WifiP2pManager、Channel、WifiP2pDevice、WifiP2pConfig
- Whisper:
  - > a pure identity-based messaging system. easy and efficient broadcasting, and also for low-level asynchronous communications.
- HOPR:
  - > a decentralized & metadata-private point-to-point messaging protocol with incentives
- MESH

# 区块链的通讯项目

- ◉ Bitphone
- ◉ Status
- ◉ Scrumble:ally
- ◉ Top
- ◉ BCM
- ◉ Voice@EOS
- ◉ Whisper@ETH
- ◉ Carrier@Elastos

# 应用场景-自主网

- ◉ Work without internet
- ◉ MESH
- ◉ Open Garden/Firechat
- ◉ goTenna/txTenna
- ◉ Helium: LongFi, Shawn Fanning, Napster
- ◉ Athea
- ◉ Bridgefy
- ◉ Slimo

# 应用场景-即时通讯-功能

- ◉ DID based
- ◉ Instant Messaging
  - > Offline Messages
  - > Group chat/broadcasting
  - > Audio/Vedio
  - > Conference
- ◉ Wallet
- ◉ <http://t.callt.net/>

# 应用场景-即时通讯-实现

- APP
- Nodes for messaging:
  - > Notify & Hold
  - > STUN/TURN
  - > Media Server
- Decentralized Storage
- Blockchain
- API

# 应用场景-邮件

- ◎ 重度依赖存储
- ◎ Stamp: stop spam
- ◎ 目录服务: email address to DID
- ◎ SMTP: Just Save to IPFS or swarm
- ◎ POP
- ◎ IMAP
- ◎ Webmail

# 应用场景-声讯服务


- ◎ 咨询，知识付费
- ◎ 有偿
- ◎ 隐私

# 去中心化通讯-挑战

- ◎ 技术
  - > 中性化系统的用户体验
  - > APP
- ◎ 市场
  - > 获取用户数
  - > 留存：子弹、多闪....
- ◎ 生态
  - > 节点数
    - 激励机制
  - > 应用数





李维 

上海 浦东新区



扫一扫上面的二维码图案，加我微信