
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
去中心化网络中的
通信反取证技术
严挺@PeerSafe

去中心化网络发展历程

去中心化网络通信反取证技术探讨

分久必合，合久必分

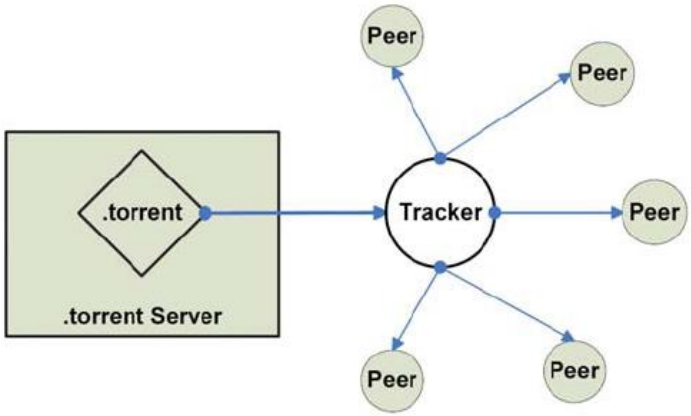
- 互联网从诞生之日起，就是去中心化的。
- 随着用户数的增多，尤其是非专业用户的大量加入，使得互联网的中心化节点越来越多。
- 随着金融业和政府/企业开始依赖互联网带来的便利，云计算和大数据使得集中化的系统达到了无法控制的地步。
- 同时，随着网络单个节点的计算能力和带宽的逐步增加，P2P的发展也开始野蛮生长。

BitTorrent

- 创始人：Bram Cohen
- 2002年10月Bram Cohen在CodeCon

发表了P2P 内容分发协议BitTorrent

- 2003年BitTorrent流行
- 每天在BT协议的基础上移动全球40%的互联网流量



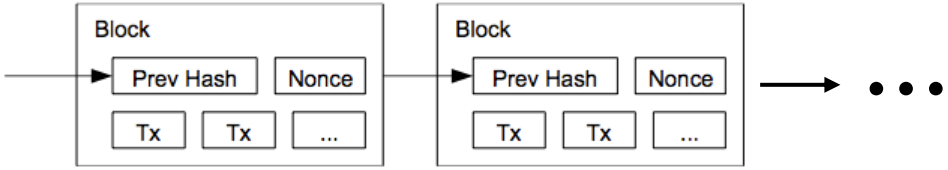
迅雷

- 2003年成立于深圳
- 创始人：邹胜龙
- 中国最大的互联网资源聚合平台
- 迅雷利用多资源超线程技术基于网格原理，能将网络上存在的服务器和计算机资源进行整合，构成迅雷网络。

新型 P2P 网络比特币

来源

- 开源 P2P 软件产生的电子货币，2009年由中本聪发明。
- 使用 P2P 网络众多节点构成的分布式数据库来确认并记录交易行为。



特点

- 完全匿名
- 无中央控制
- 交易成本低廉

第一个成功的去中心化网络商用系统

莱特币

莱特币受到了比特币（BTC）的启发，并且在技术上具有相同的实现原理，莱特币的创造和转让基于一种开源的加密协议，不受到任何中央机构的管理。

对比特币的改进：

- 每2.5分钟就可以处理一个块，因此可以提供更快的交易确认
- 莱特币网络预期产出8400万个莱特币，是比特币的4倍
- 挖掘更为容易

可以帮助用户即时付款给世界上任何一个人

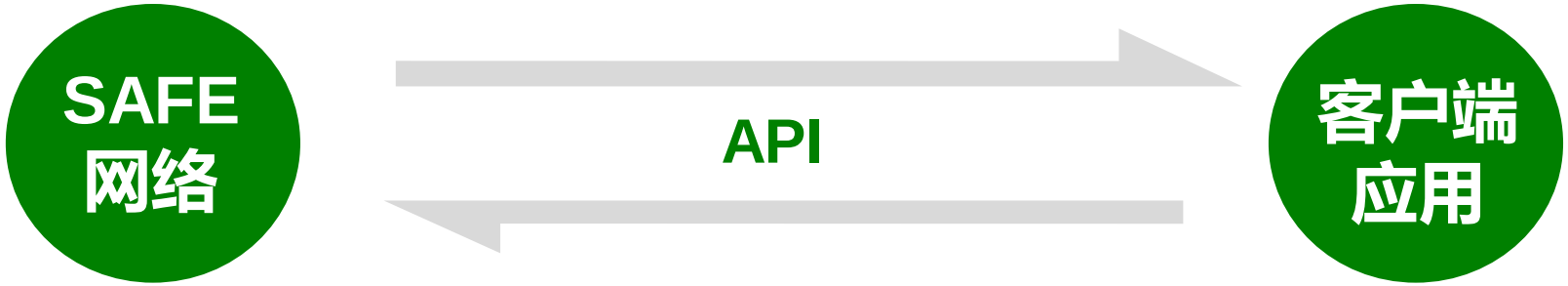
Ripple去中心化支付网络

Ripple是世界上第一个开放的去中心化支付网络

- 支持多种货币
- 自动进行汇率换算
- 交易确认过程可在几秒钟内完成
- 客户端不需要下载区块链
- 无需也不能挖矿
- 需要维护一个包含所有帐号、所有交易的总帐本

去中心化全货币金融体系

MaidSafe去中心化网络平台



完全分布式的数据管理服务

1. 由节点贡献资源构成分布式服务器系统
2. 管理静态数据、动态数据以及通信
3. 完成传统网络提供的httpd，SSH，FTP，SMTP，SCP，POP3，IMAP等功能

去中心化应用

1. 自我加密、认证实现安全接入
2. 对网络进行安全访问，存储，修改和通信操作
3. 提供许多在中心化结构网络下不能实现的服务

目前还处在实验开发阶段

去中心化网络发展历程

去中心化网络通信反取证技术探讨

中心化通信APP反取证技术

Snapchat

开发商：美国Snapchat

- 主打阅后即焚
- 快速分享图片
- 出现过照片外泄事故
- 最近推出收费回放业务

支持平台:
iOS,Android,PC

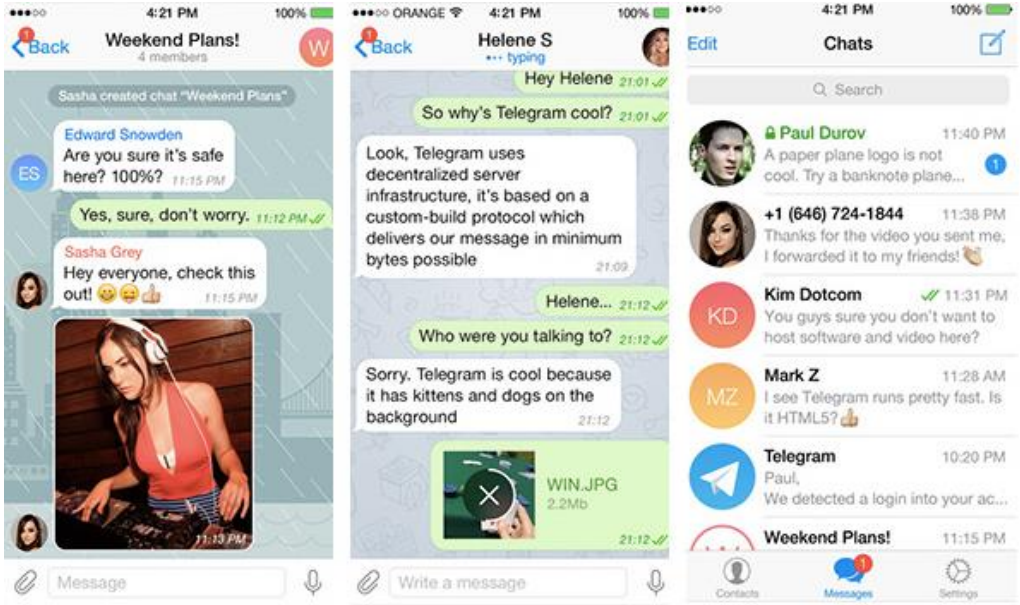
中心化通信APP反取证技术

Telegram

开发商：俄罗斯Telegram

- 端到端加密
- 号称基于去中心化网络
- 消息在服务器定时删除

支持平台:
iOS,Android,PC



中心化通信APP反取证技术

Wickr

开发商：美国Wickr

- 采用军事级别加密技术
- 无痕迹通信
- 无广告应用

支持平台:
iOS,Android,PC

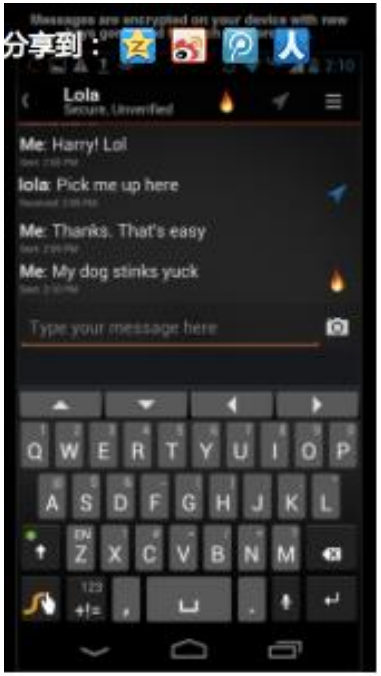
中心化通信APP反取证技术

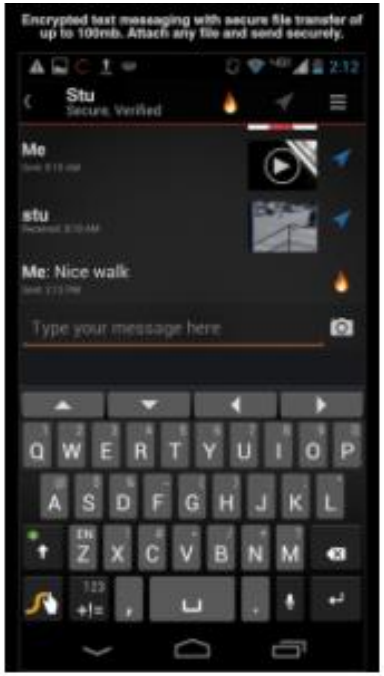
Silent Text

开发商：瑞士Silent Circle

- P2P协议
- 阅后即焚
- 支持大文件加密发送

支持平台:
iOS,Android





中心化通信APP的比较

功能	Snapchat	Telegram	Wickr	Silent Text
P2P 通信	✖	✖	✖	✔
E2E 加密	✖	✔	✔	✔
阅后即焚	✔	✔	✔	✔
无网通信	✖	✖	✖	✖
无需注册	✖	✖	✖	✖
多平台支持（iOS,Android, PC）	✔	✔	✔	✖

去中心化通信APP反取证技术

FireChat

开发商：美国Open Garden

- P2P协议
- 无网络可利用机身WiFi或蓝牙通信
- 支持网状网络

发展历史：

- 2014年3月份问世后一举占领了运营商不靠谱的印度和地震频发的日本
- 2014年6月伊拉克陷入内战后随即走红
- 2014年9月香港占中一天增加10万用户

支持平台:
iOS,Android,PC

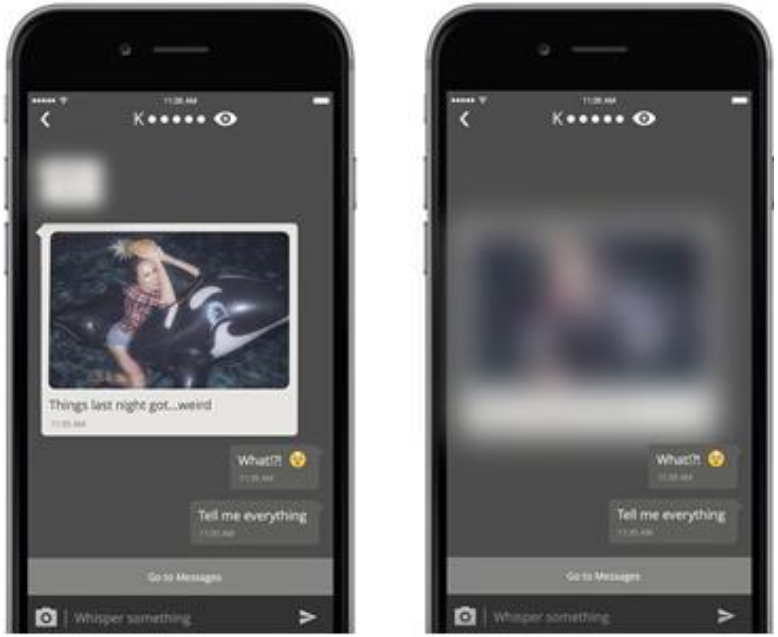
去中心化通信APP反取证技术

Bleep

开发商：美国BitTorrent

- P2P协议
- 信息不通过服务器端
- 端对端加密协议
- 支持无注册隐身模式
- 支持阅后即焚

支持平台:
iOS,Android,PC



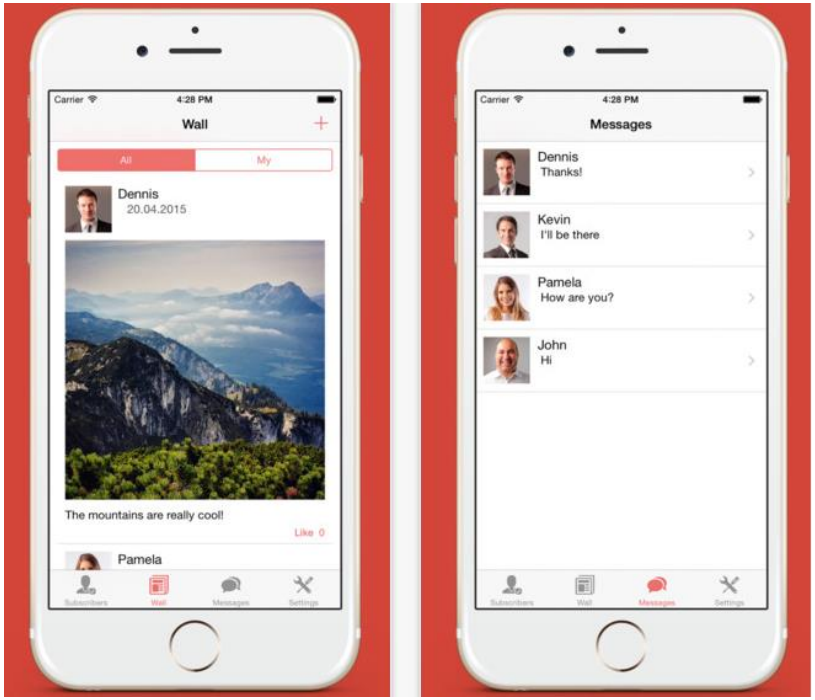
去中心化通信APP反取证技术

CheChat

开发商：俄罗斯**AppCraft OOO**

- P2P协议
- 信息不通过服务器端
- 端对端加密协议
- 用户注册无需提供个人信息
- 可随时更换ID
- 支持私密朋友圈

支持平台:
iOS,Android



去中心化通信APP反取证技术

ShadowTalk

开发商：新加坡 PeerSafe

P2P
- 真正的点对点
- 无中心服务器

无需注册
- 无需个人信息
- 无用户名密码

从不存储
- 阅后即焚
- 无证可取

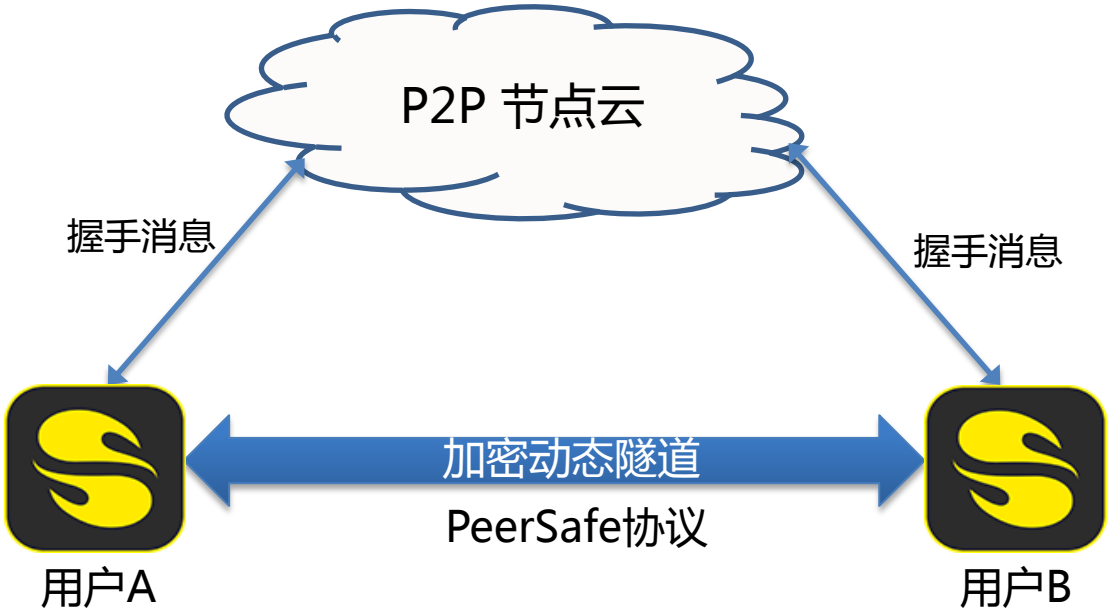
全程加密
- 端到端加密
- 逻辑关系打乱

支持平台:
iOS,Android,PC

去中心化通信APP的比较

功能	FireChat	Bleep	CheChat	ShadowTalk
P2P 通信	✔	✔	✔	✔
E2E 加密	✔	✔	✔	✔
阅后即焚	✖	✔	✖	✔
无网通信	✔	✖	✖	✔
无需注册	✔	✔	✔	✔
多平台支持（iOS,Android, PC）	✔	✔	✖	✔

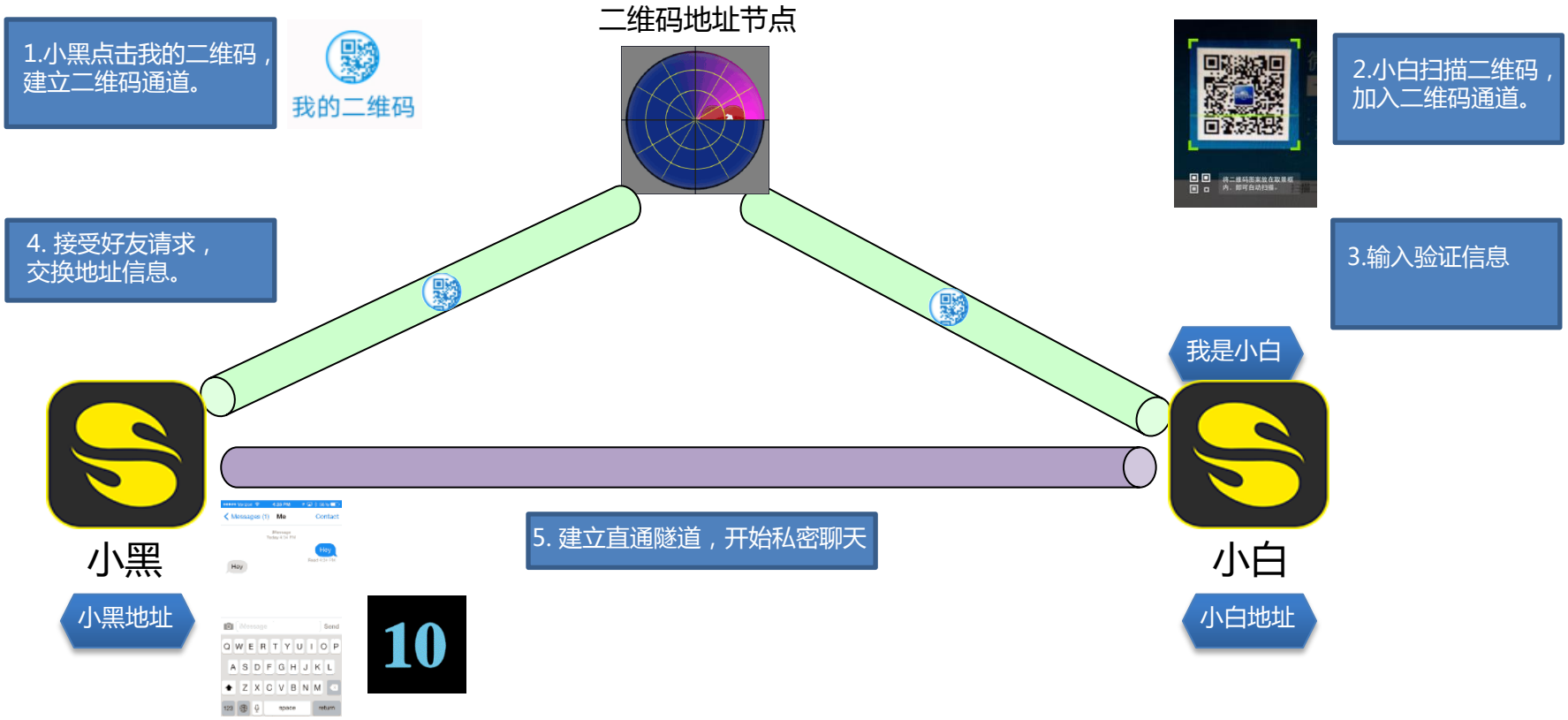
ShadowTalk通信原理



1.用户之间通过 P2P 节点云建立加密连接
2.用户通过加密动态隧道传输私密信息

ShadowTalk通信建立过程

小黑刚刚安装了ShadowTalk APP，想和小白私密聊天。



个人参与自由搭建的随机网络

个人电脑、路由器安装 ShadowTalk 接入SDK后相当于二维码节点服务器

- 可以和 ShadowTalk 移动端APP 联动
- 能绕过中心化网络和其他 ShadowTalk 终端通信，无法取证通信内容
- 能避开网络实名制取证
- 能躲开大数据收集取证

- 本地可开展阅后即焚内容服务，该内容不属于任何服务商，取证难度高。

问题求证

随着移动设备能力的增强，网络速度的加快，去中心化网络通信正向我们走来。

对于这样的新一代的去中心化网络通信，我们如何进行电子取证？

抛砖引玉

1）各种输入法尤其是第三方输入法的入口
2）第三方插件，包括各种监控系统的集成SDK
3）P2P网络节点的数目控制
4）其他全网监控方式

关于PeerSafe

- 2014年7月成立
- 重点研究P2P网络安全和协议自组网
- 提出了随机去中心化网络通信协议
- 研发了P2P加密通信软件ShadowTalk
- 研发了分布式身份认证系统
- 这些系统和后续开发的成果已经开始商用

欢迎合作
谢谢！

邮箱：yanting@peersafe.cn
网站：www.peersafe.com