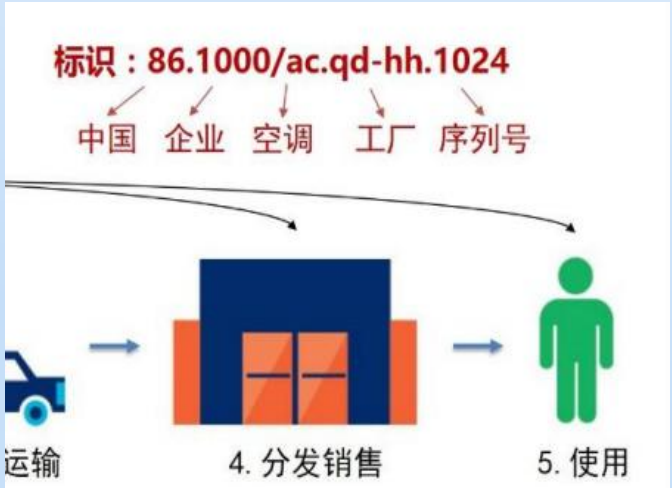
万物如何互联

道里名服务系统
DaoliNameService DNS

DaoliName
2019年五月

万物互联前提：万物须可认

- 史前迄今：万物可认需求历久弥新：父传姓、人取名、户入籍、地编址、图书馆学、仓库管理、域名服务、...
- 1992年：DARPA-CNRI 提出了Handle System思想，1994年：实现了DOI（Digital Object Identifiers）
- 2003年：IETF Handle System 标准化工作
  - RFC3650 Handle System Overview
  - RFC3651 Handle System Namespace and Service Definition
  - RFC-3652 Handle System Protocol (ver 2.1) Specification
- 2017年：



- 共性需求：*有构造，易查询，可规模管理*

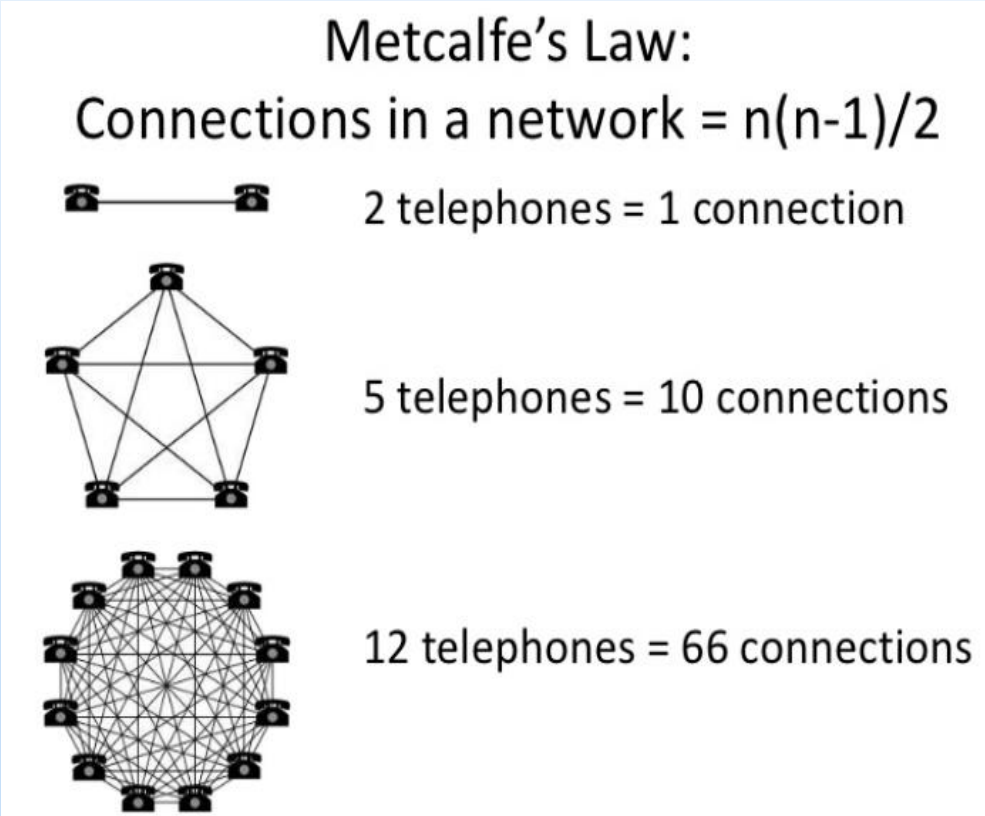
万物 peer-to-peer 直连乘积效应

一个电话是毫无用处的

两个电话就很有用，难怪密码学家津津乐道于此场景研究，怎么保护 Alice，Bob 永远谈不完的话

Metcalfe's Law: n个电话p2p互联，产生的有益效果 = n^2，连接设备越多，网络效益越大

仅当电话号码的管理是有条不紊的，规模才越大越好，右图电话号码若无构造，管理可以是噩梦

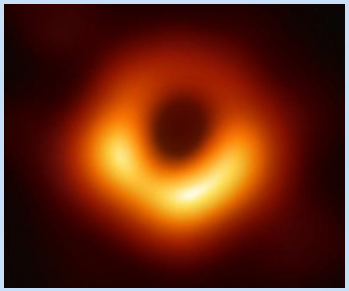


2019年热点需求：万物须安全可认

万物皆已智，可操作密码学算法实现安全认证，公钥体制：n 设备互认管理复杂度 = n，臻达最优！

- 传统公钥体制：随机私钥 → 随机公钥，比特币，区块链皆如此，封闭系统中 peer node 用随机身份 is not a problem，可 feature 匿名：谁是中本聪？p2p = r2r (r = random) 身份就是要随机

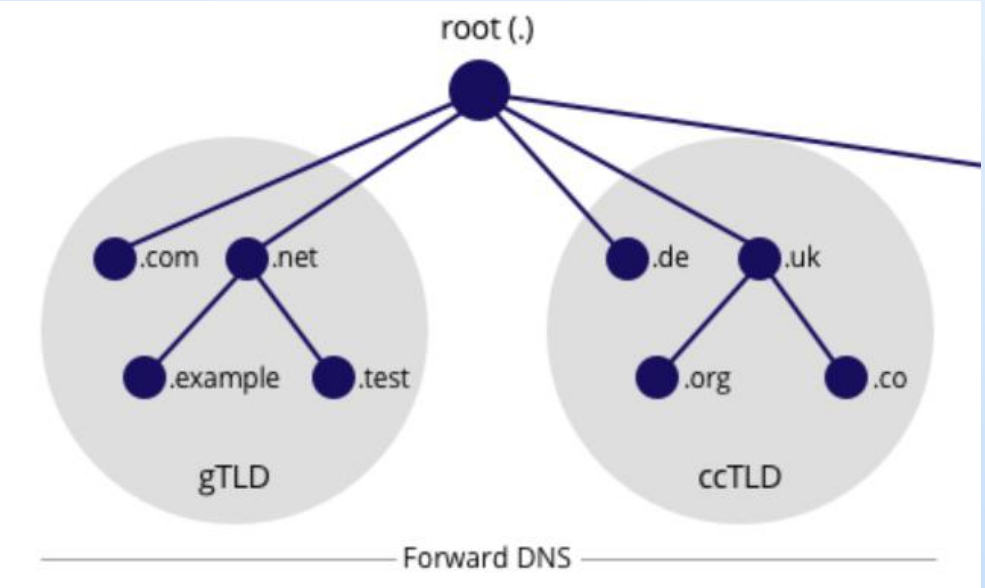
- 一个开放系统则须对设备身份实施公开管理：传统PKI，CA为每一设备颁发证书，将***有构造，易查询，可规模管理*** 的设备身份与随机公钥绑定，无条件信任CA，证书含（可能巨量）史上已吊销证书，请勿被右图迷惑，迄今 PKI 并未赢得客户端青睐，哪位看官有公钥证书的请举手？



- 基于身份的公钥体制（IBC）：有构造，可查询，易管理的身份即公钥，然而私钥须由系统中心生成，此私钥生成中心成为系统安全脆弱黑洞，IBC 2000 年发明迄今被束之高阁之缘由？

道里名身份即公钥服务

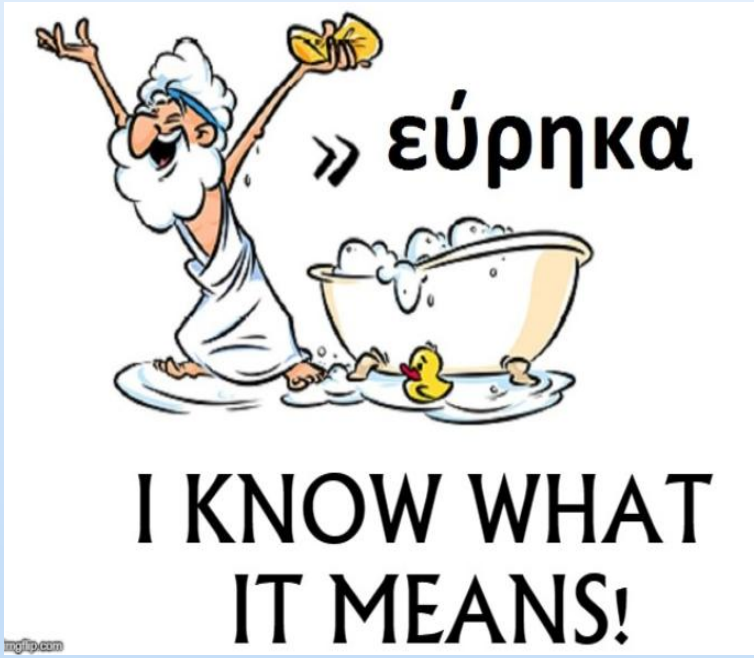
- 受启发于域名服务系统DNS：互联网服务器域名：***有构造，易查询，可规模管理***，DNS全球范围管理域名，提供查询服务，将域名绑定颇为随机的IP地址, DNS构造：



- DNS是个交互式询问-应答服务系统，传销式服务构造形成极高管理效率，规模可巨大扩展，且服务具有天然垄断性，行业垄断者：Verisign

道里名身份即公钥服务

- 考虑域名 = 公钥，客户端可验证 IP 绑定正确性，应用 IBC 可有效解决 DNS 安全问题
- 从 DNS 询问-应答机制进一步观察：返回 IP 亦可作公钥，此公钥看似随机，却可用 bilinear pairing 验证与域名绑定为真
- 那么问题来了：再多此一举 “IP” 作为公钥，何贵干之有？
- Eureka！此公钥关联之私钥不必再由系统中心生成！
- 系统范围深不可测之集中风险可分散消减了！



区块链认证的, Peer-to-Peer, 身份即公钥

身份即公钥 ID as a Public Key (IDaaPK)

- 邮箱地址, 手机号, 社交网络账号, ..., 你所选的任意字符串, 仅当唯一并为你所有, 皆可注册成为你的公钥
- 身份即公钥: 可用于加密, 但用于解密却是无效的
- 你的APP: 私人独享私钥设备方可解密

道里名身份即公钥注册管理服务系统

- DNS（Daoli Name Service）
  服务系统不处理任何秘密
- 无“脱裤”风险，无单点失效
- 服务规模可分布弹性扩展

零信任, 分布式共识机制

- 区块链认证的 IDaaPK 公钥
- 无人可更改区块链上存的 IDaaPK 公钥
- 无证书, 无CA认证中心
- *去除私钥生成中心的* SM9 ISO 标准
- Peer-to-peer, 如手机到手机, 私有安全信道, 如社交网络之上的虚拟私有网络

未来是私人的，因为今天是手机的

DAOLI NAME

马上就试！ http://47.94.83.10/daoliname.apk

Android only for the moment, other OSes soon