DAOLI NAME

How to Connect Smart Dusts

DaoliName Service

May 2019

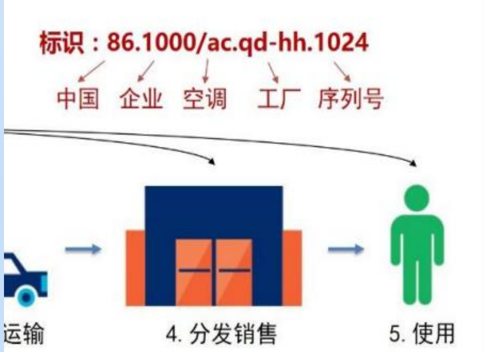
Smart Dusts Connect?
May I know your name dust?

- Once upon a time, like father like son in the name of, ..., postcode, library study, inventory management, ..., domain names, ...
- 1992: DARPA-CNRI proposed “Handle System”
- 1994: DOI (Digital Object Identifiers) implementation
- 2003: IETF Handle System RFCs
  - RFC3650 Handle System Overview
  - RFC3651 Handle System Namespace and Service Definition
  - RFC-3652 Handle System Protocol (ver 2.1) Specification
- 2017: Chinese IoT Name Resolution Whitepaper

工业互联网产业联盟
Alliance of Industrial Internet

工业互联网标识解析—
产品追溯白皮书

（2017年）



Common Need: Good IDs = structured, can be scalably managed

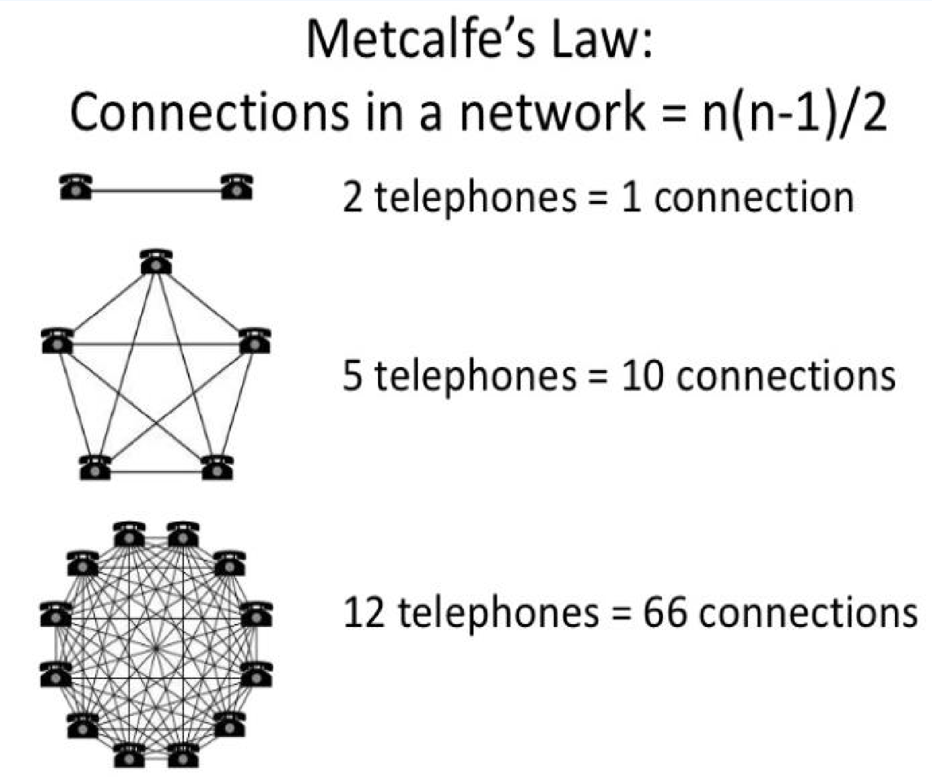
Peer-to-peer Connection Multiply^2

One phone is useless

Two phones are very useful, no wonder cryptographers are so addicted to study Alice and Bob

Metcalfe's Law: n phones p2p connection = n^2 multiply revenue for, e.g., “The Phone Company”

However unless phone numbers are structurally organized, line plugging girls would have been in nightmarish job



Metcalfe’s Law:

Connections in a network = n(n-1)/2

2 telephones = 1 connection

5 telephones = 10 connections

12 telephones = 66 connections

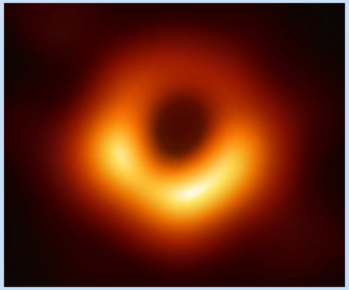
Mandate Starting 2019: Smart Dusts Must Know Each Other Securely

With dusts already smart, crypto does authentication
Public Key: n nodes authentication complexity = n

- Because random private key → random public key, in a close system, e.g., BTC, blockchain, peer node having random ID features anonymity! Who is Nakamoto? p2p = r2r (r = random)

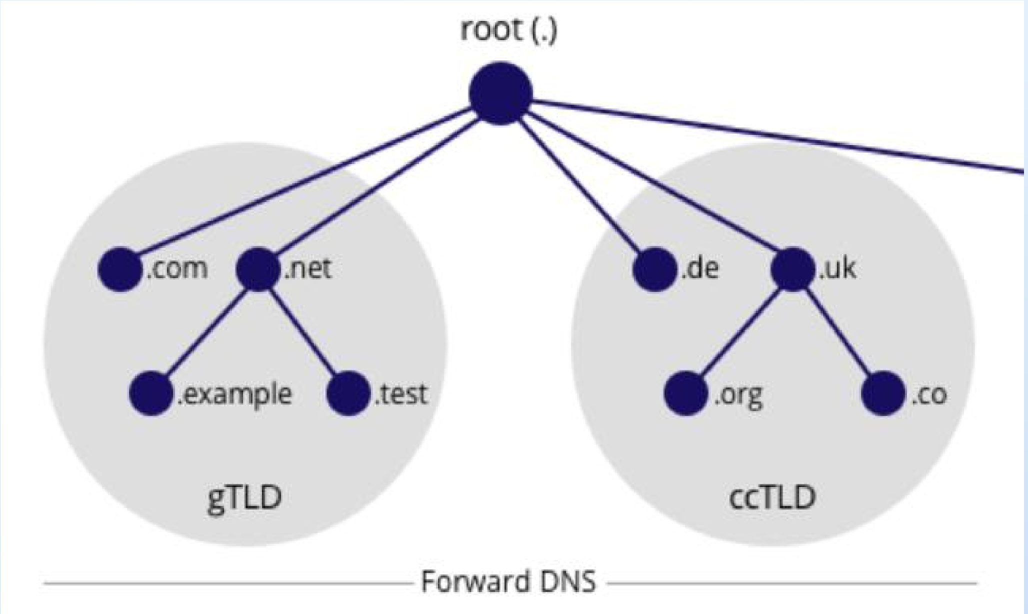
- Open system must use good IDs. PKI: CA binds a good ID to random pub key. A cert may include all revoked certs in the history. PKI has never won clients (Trust CA, not the figure in the right!)

- Identity Based Crypto: A good ID is a public key! Need Private Key Generator (PKG), centralized gravity for attacks! Why not seen any semblance of impact since a promising proposal in 2000?



An Example of Good IDs

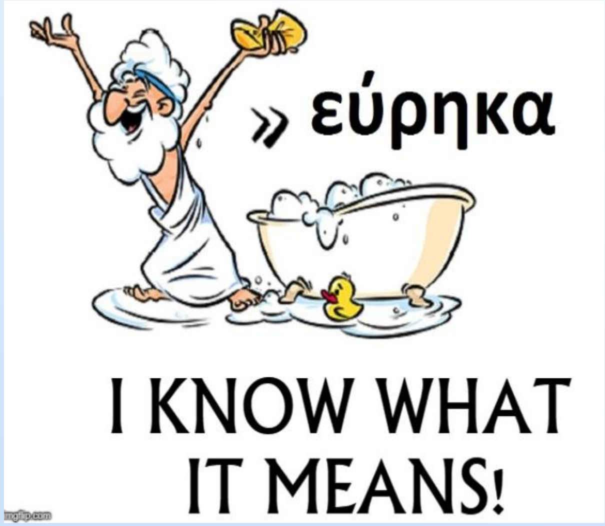
Domain Names: well structured, globally searchable, DNS binds DN to more random looking IPs



DNS is an interactive query-answer system, pyramid sale structure and management efficiency, and the service enjoys natural monopoly

ID as a Public Key (IDaaPK) Inspiration

- Consider a DN = public key, a client can verify binding (DN, IP). IBC can offer a good DNS security solution
- Observe, a returned IP can also be a public key, though looking random, bilinear pairing can verify the binding
- Q: What is one more IPaaPK for?
- Eureka! The private key behind this IPaaPK needn't be generated by PKG anymore!
- The centralized gravity for attacks is dispersed



DaoliName IDaaPK Service

Distributed consensus ledger fixation of "Trustlessly Agreeable Diffie-Hellman Quadruple" (TADHQ)

- TADHQ is publicly verifiable by evaluating bilinear pairings inputting (IDs, IDaaPKs) as elliptic curve points
- No one can alter the TADHQ fixation once entering the ledger
- No CA, no PKG, no centralized single point of attack or failure
- Peer-to-peer, e.g., mobile phone VPN overlaying social network
- Service handles no secret and can be easily elastically scaled in world wide distributed replicas

No Central Authority

The Future is Private but NOT Centralized

DAOLI NAME

Try it NOW! http://47.94.83.10/daoliname.apk
Android only for the moment, other OSes soon