



DA 福 LI NAME

Blockchain Authentication for Smart Dusts

DaoliName Service

May 2019

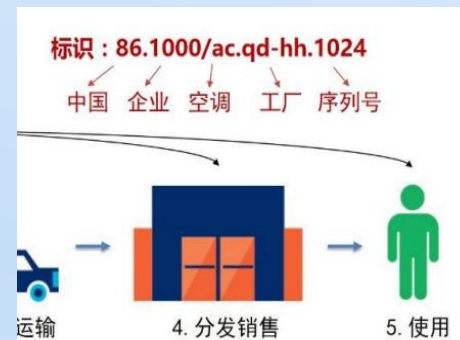


Authentication for Smart Dusts?

May I know your name dust?



- Once upon a time, ..., family name, ..., Tel no, library study, postcode, inventory, ..., domain names, email address, URL, ..., You name it!
- 1992: DARPA-CNRI proposed “Handle System”
- 1994: DOI (Digital Object Identifiers) implementation
- 2003: IETF Handle System RFCs
 - RFC-3650 Handle System Overview
 - RFC-3651 Handle System Namespace and Service Definition
 - RFC-3652 Handle System Protocol (ver 2.1) Specification
- 2017: Chinese IoT Name Resolution Whitepaper



What's in common: GoodIDs = universally uniquely identifiable, structured, meaningful for human, scalably manageable

Peer-to-Peer Connection Multiply²

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 connected = n^2 multiply
revenue for, e.g., “The
Phone Company”

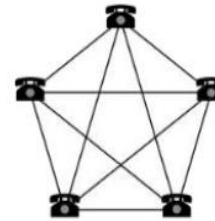
However unless phone
numbers are structurally
organized, line plugging girls
would have been in
nightmarish job

Metcalfe's Law:

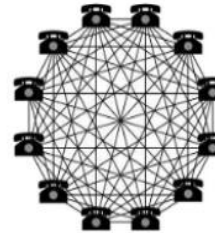
Connections in a network = $n(n-1)/2$



2 telephones = 1 connection




5 telephones = 10 connections

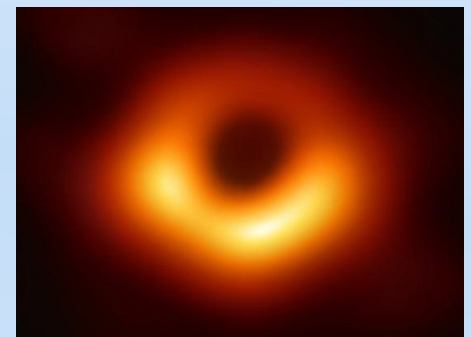


12 telephones = 66 connections

Mandate From 2019: Smart Dusts Must Know Each Other Securely

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

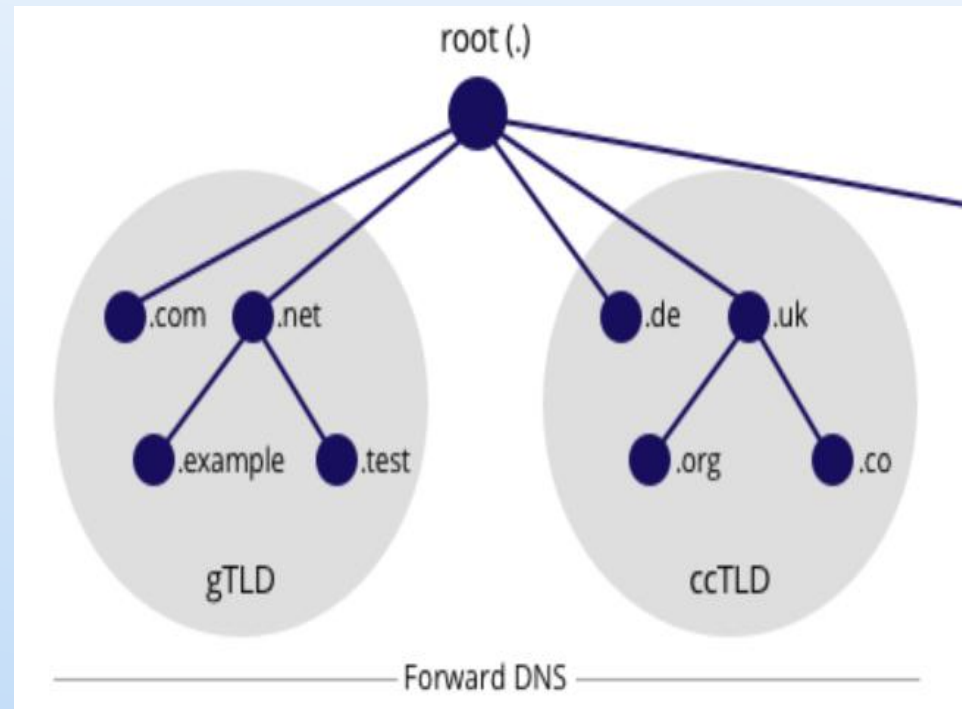
- With random private key \rightarrow random public key, in a close system, e.g., BTC, blockchain, peer nodes having random ID features anonymity!
Who is Nakamoto? $p2p = r2r$ ($r = \text{random}$)
- PKI: CA binds a GoodID to a random public key. A cert may be huge to have all revoked certs. PKI has never won clients, let alone mobiles (Trust CA, not the figure in the right!)
- PGP: 1st Amendment free export RSA! 
- Identity Based Crypto: GoodID is public key! Need Private Key Generator (PKG). Centralized gravity for attacks! Why no semblance of impact since a promising proposal in 20 years ago?



An Awesome Example of Managing GoodIDs

Domain Names: Well structured, global scale searchable, DNS binds DN as a GoodID to a more random looking IP

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



GoodID as a Public Key (IDaaPK)

Inspiration from Interaction

- 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!
- Centralized gravity for attacks and single point failure is dispersed



Trustlessly Agreeable Diffie-Hellman Quadruple Membership Decision



Bilinear Pairing, bilinearity easily computable

$$\hat{e}(U + V, U') = \hat{e}(U, U') \times \hat{e}(V, U')$$

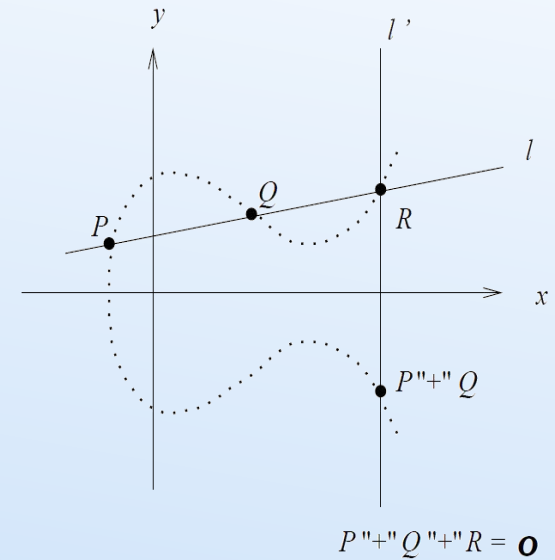
$$\hat{e}(U, U' + V') = \hat{e}(U, U') \times \hat{e}(U, V')$$

Let $Alice_1, Alice_2$ be “pairing friendly elliptic curve” points which are deterministically derived from Alice's GoodID. The following pairing equation is publicly decidable, i.e., Trustlessly Agreeable.

Decision making does not need to know Alice's private key k_{Alice}

$$\hat{e}(Alice_1, [k_{Alice}]Alice_2) = \hat{e}([k_{Alice}]Alice_1, Alice_2)$$

($Alice_1, Alice_2, [k_{Alice}]Alice_1, [k_{Alice}]Alice_2$) is called Trustlessly Agreeable Diffie-Hellman Quadruple (TADHQ). Publicly decidability of TADHQ means it contains ONLY GoodID. Entering TADHQ in a public blockchain service, GoodID is publicly agreeable being cryptography worthy public key(s).



DaoliName Service for IDaaPK



Distributed consensus ledger fixation of TADHQ for IDaaPK:

- No one can alter TADHQ, i.e., GoodID based IDaaPK, fixation once entering a distributed consensus 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
- IDaaPK uses ID-asking, IDaaPK-answering online service, so it has inherent key revocation (Who can live offline today, not even a cryptographer!)



Applications

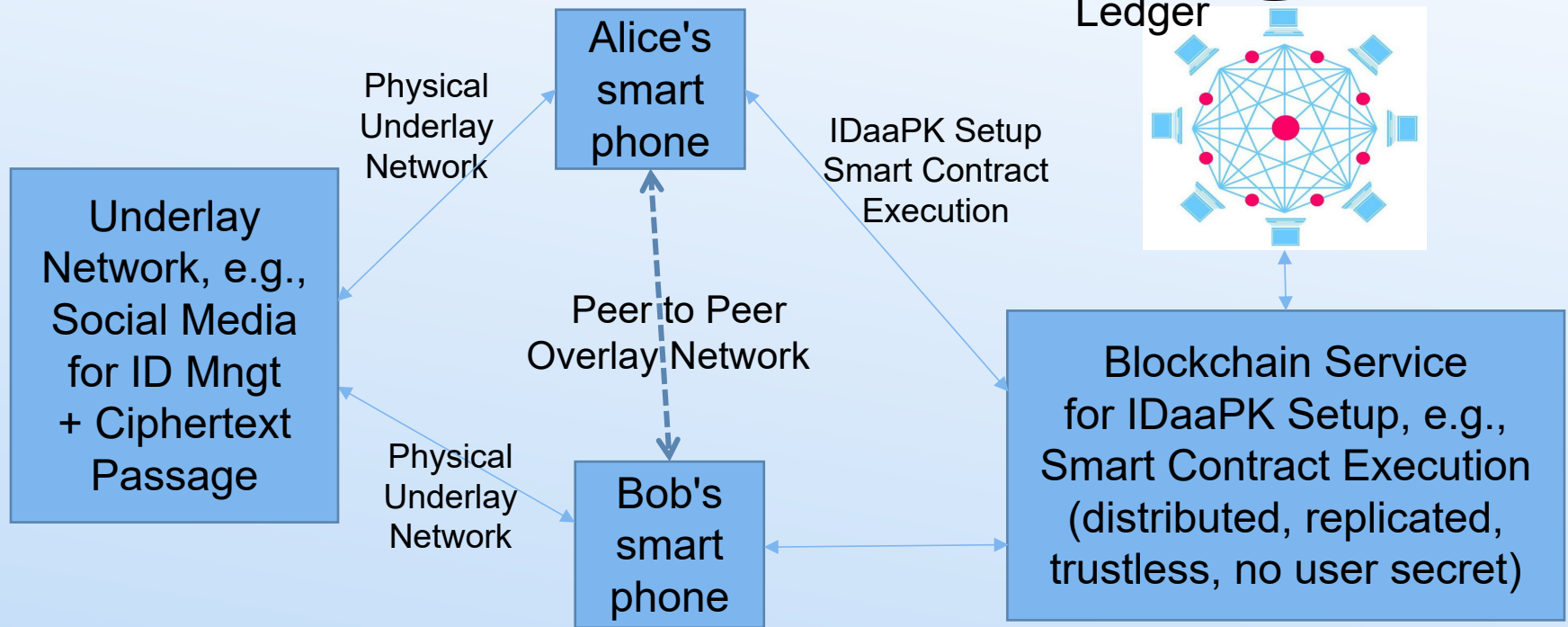
- DNs are GoodIDs, IPs bound to DNs are GoodIDs too, therefore SSL like web security can straightforwardly use IDaaPK: No CA, no cert, no muss, no fuss
- IPsec VPN: No CA, no cert, off you go!
- Clients IDaaPK: SSL two-way authentication for the first time
- Overlay “VPN” on top of social media network as underlay, e.g., secure, private, business and office uses of WeChat, Facebook, and the like
- IoT security, ...



Try it NOW!

IDaaPK “VPN” overlay social media network
<http://daoliname.com:8080/daoliname.apk>

IDaaPK “VPN” Overlay: Explained



A Smart Contract Example:

Party A: Alice's smart phone with social media account “Alice” = GoodID

Party B: The World

Contract Content: “Alice”, TADHQ = (Alice₁, [k_{Alice}]Alice₁, Alice₂, [k_{Alice}]Alice₂)

Screen shot of Alice timely showing-off on her social media

Contract Output: 1: Hash of Contract Content entering the Blockchain

2: Private key k_{Alice} establishing in Alice's smart phone

The Future is Private AND NOT Centralized



DAOLINAME

Try it NOW! IBC for smart phones
<http://daoline.com:8080/daoline.apk>
(Android for the moment, other OSes soon)