



DA 福 LI NAME

DaoliNameCoin

A Uniquely Novel Blockchain

Squared Zooko's Triangle

DaoliName Service
June 2019

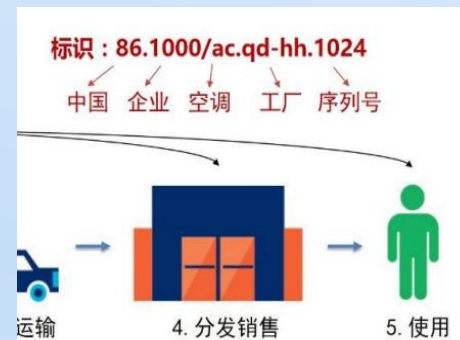


Authentication for Smart Dusts?

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”

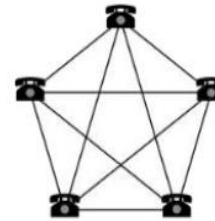
However unless phone
numbers are structurally
organized, line plugging girls
would have been in
nightmarish job

Metcalfe's Law:

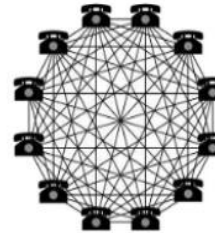
Connections in a network = $n(n-1)/2$



2 telephones = 1 connection



5 telephones = 10 connections




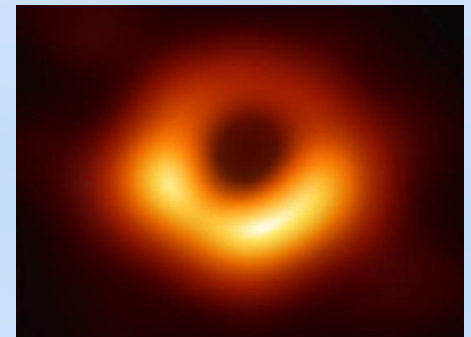
12 telephones = 66 connections

Mandate From 2019: Smart Dusts Must Know Each Other in Authentication



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?



Zooko's Triangle for ID Authentication

My WeChat ID binding to an address can ONLY enjoy 2 out of the following 3 usefulness:

<http://wechat.com/f6b9ef03e8b...f71c3>:

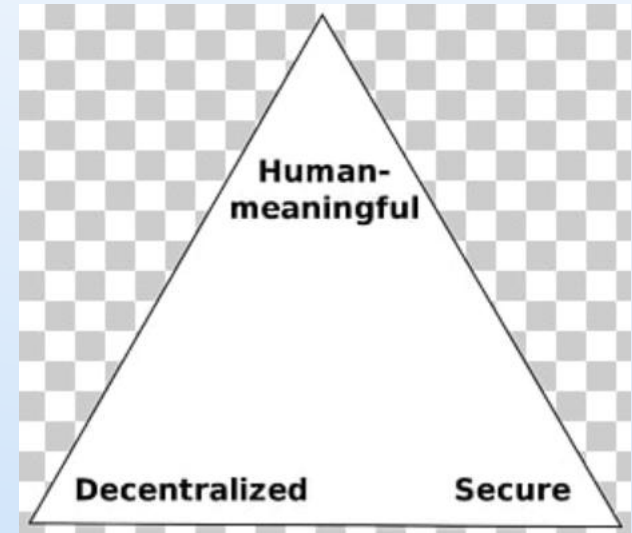
Putting this ID = address to a public blockchain, the (ID, address) binding is decentralized secured, but the ID is *not human meaningful*, i.e., not a GoodID

http://wechat.com/wenbo_mao:

Signing to bind this GoodID to an address, with a certificate issued by, e.g., DNSSEC, (ID, address) binding is secure but must trust a *centralized* CA root

DNS no SEC can also binds the above GoodID to an *insecure* address

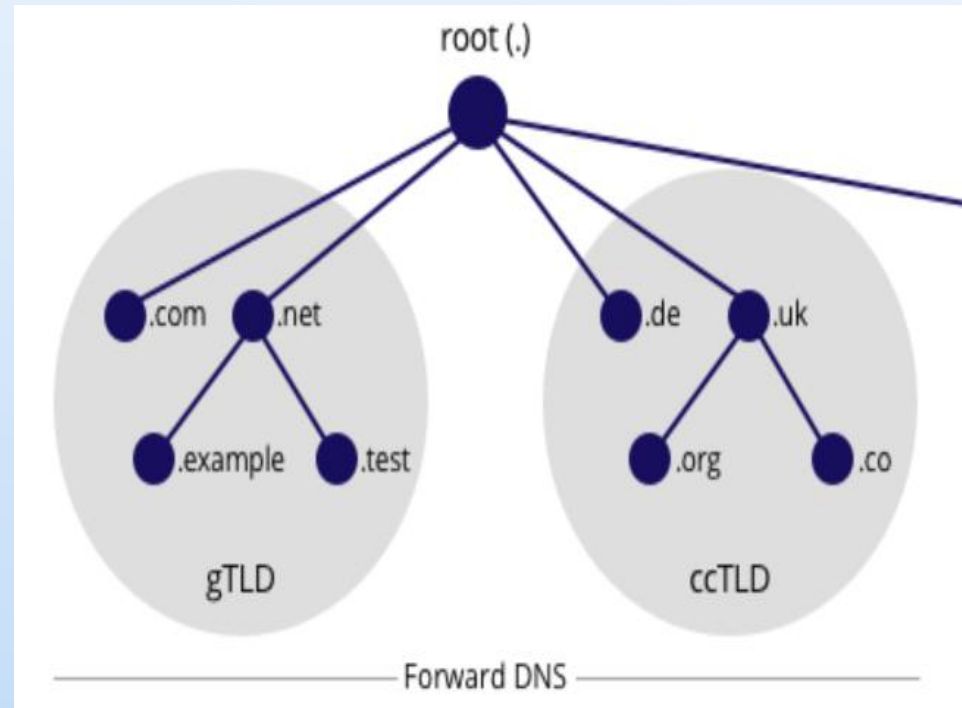
Zcash founder Zooko Wilcox-O'Hearn made this “Pick 2 only” conjecture



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 (IDPK) 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 IDPK for?
- Eureka! The private key behind this IDPK 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

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

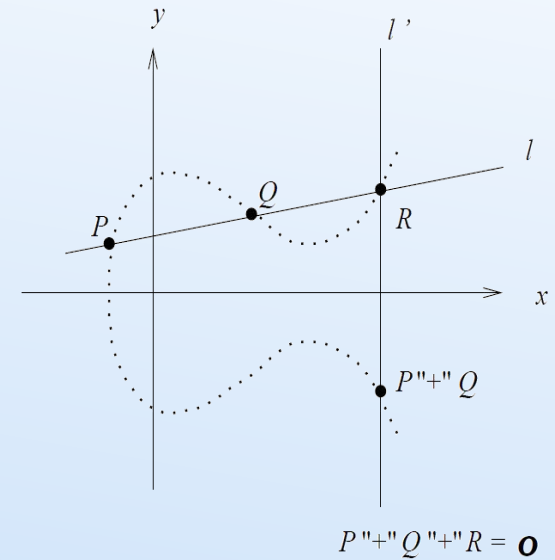
$$\hat{e}(U, U' + V') = \hat{e}(U, U') \times \hat{e}(U, V')$$

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).



Zooko's Triangle: No More a Trilemma

Version 1

Let Alice have a blockchain wallet,
with the wallet's private key being k_{Alice}

Using her wallet's private key and
GoodID, Alice can construct TADHQ:
(Alice₁, Alice₂, [k_{Alice}]Alice₁, [k_{Alice}]Alice₂)



By destroying anonymity for her blockchain address,
Alice gains advantage of enjoying “squaring” Zooko's Triangle!
Alice's blockchain wallet provides authentication for binding
her GoodID and her blockchain address, trustlessly

In this preliminary version, Alice's GoodID may be stolen by
somebody in 1st-come-1st-serve manner: it remains secure
for that blockchain wallet owner

DaoliName Service for IDPK



Distributed consensus ledger fixation of TADHQ for IDPK:

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



Applications

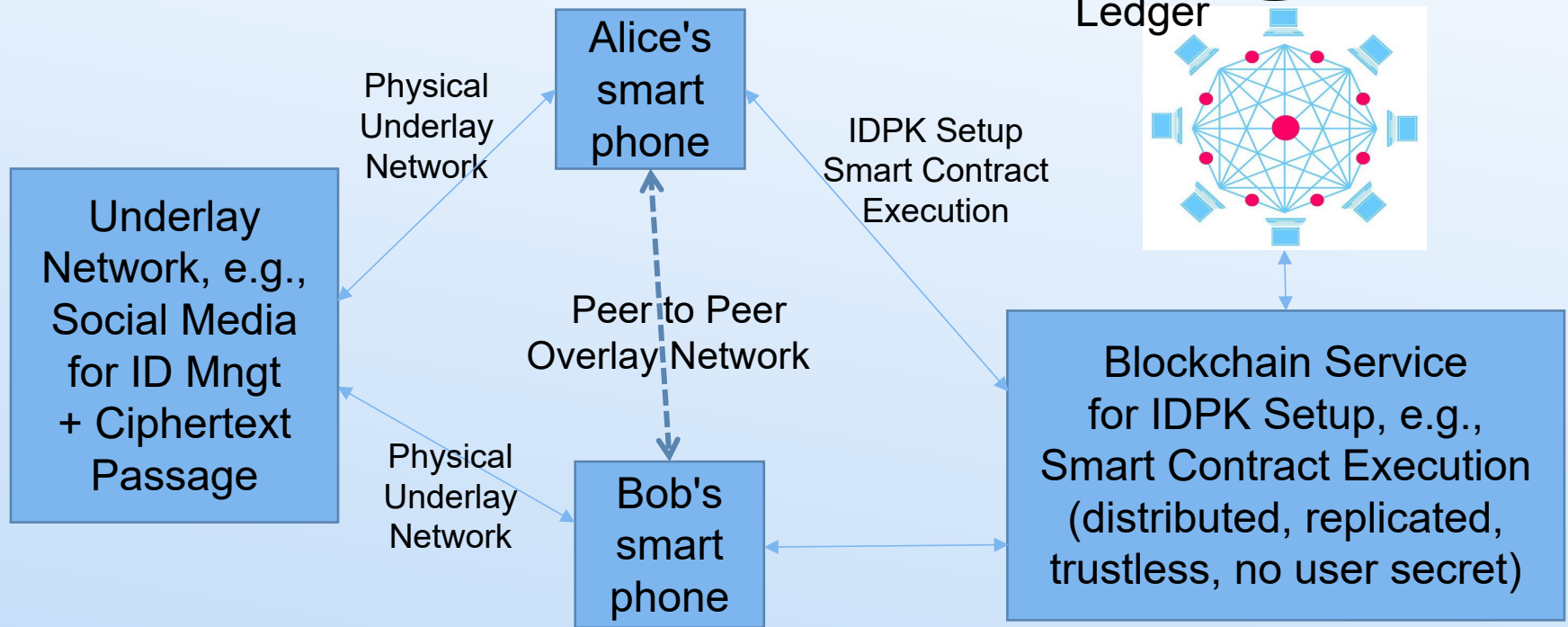
- DNs are GoodIDs, IPs bound to DNs are GoodIDs too, therefore SSL like web security can straightforwardly use IDPK: No CA, no cert, no muss, no fuss
- IPsec VPN: No CA, no cert, off you go!
- Clients IDPK: SSL two-way authentication for the first time
- Overlay “VPN” on top of social media network as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



Try it NOW!

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

IDPK “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

Improving “Smart Contract” Content

In the “social media timely showing off” example, “timely” can include a challenge response mechanism, and “showing off” can be Alice persuading her friends to flatter her. These are designed to add difficulties to GoodID theft

Let Bob be an old acquaintance of Alice, the following bilinear paring equations are trustlessly verifiable

$$\hat{e}([k_{\text{Bob}}]\text{Alice}_1, \text{Bob}_2) = \hat{e}(\text{Alice}_1, [k_{\text{Bob}}]\text{Bob}_2)$$

$$\hat{e}([k_{\text{Bob}}]\text{Bob}_1, \text{Alice}_2) = \hat{e}(\text{Bob}_1, [k_{\text{Bob}}]\text{Alice}_2)$$

1. Bob has already registered his IDPK, the following TADHQ $(\text{Bob}_1, [k_{\text{Bob}}]\text{Bob}_1, \text{Bob}_2, [k_{\text{Bob}}]\text{Bob}_2)$ is already in the ledger;
2. Bob is introducing Alice to Registrar by using his private key to sign Alice's GoodID, in exactly the way of PGP Web-of-Trust

Registrar can demand Alice to submit several PGP Web-of-Trust helpers signatures, for “Alice” being more and more likely her own GoodID



Evolution from PKI CAs to IDPK

Examples of Fully Qualified Domain Names (FQDN):

www.microsoft.com

research.microsoft.com

asia.research.microsoft.com

ai.research.asia.microsoft.com

...,

Let a FQDN be DNS service
bound to an ip address IP

Let the owner of (FQDN, IP)
use a private key k to construct TADHQ as follows:

(FQDN, $[k]$ FQDN, IP, $[k]$ IP)

Let (FQDN, IP) owner display TADHQ on a `https://FQDN` webpage

Let IDPK server ping FQDN, upon response IP matching that in TADHQ,
enter TADHQ + webpage screenshot + ping screenshot in the ledger

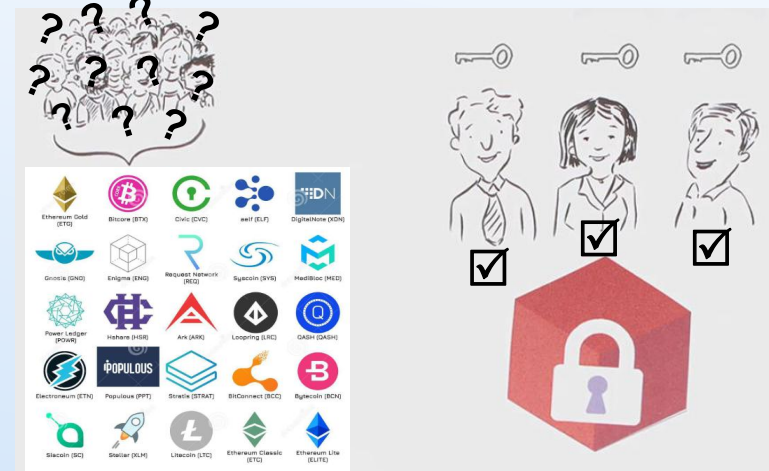
This is to evolve PKI CA based SSL to IDPK based SSL. Open source
IDPK SSL will soon be available. Keep tuned!



DaoliNameCoin: A Unique Blockchain



Using bilinear pairing friendly elliptic curve, in specific, BN512 curve, $G_1 \times G_2 \rightarrow G_T$ where G_1 is a “crypto curve” as normal as in all existing blockchains; G_2 is uniquely novel in blockchain technology, for GoodID use; G_T is for verifying pairing use (novel too, but no need boasting)



Let P be a system public point in G_1 , let a denote Alice's private key; Alice first joins DNC anonymously as in all existing blockchains; for this normal use, she only needs using G_1 ; her public address is $[a]P$

Some Alices may choose to become known in their GoodIDs; such an Alice makes G_2 transaction to link her anonymous address to Alice:

$$\text{TADHQ} = (P, [a]P, \text{Alice2}, [a]\text{Alice2})$$

A Proof-of-Stake (PoS) club member nodes verify smart contracts, e.g., cloud email, social media, DN-IP binding, etc., upon reach not-ID-theft consensus, Alice can enjoy no-muss no-fuss use of GoodID-PK

The Future is Private AND NOT Centralized



DA^名LI NAME

Stay Tuned for DaoliNameCoin Soon to Launch!