The Decentralized Identifier (DID) in the DNS

draft-mayrhofer-did-dns-00

A. Mayrhofer (nic.at) - D. Klesev (nic.at) - M. Sabadello (danubetech)
alexander.mayrhofer@nic.at
IETF 103, Bangkok, TH
Background (1) – Blockchain Adressing

• „Distributed Ledgers“ (read: Blockchains) typically use Addresses to identify resources
  • 3E53XjqK4Cxt71BGeT2VhpcotV8LZ853C8

• Problem A: Interopability
  • Which ledger is this address?
  • Trial & Error?
  • (above example is a bitcoin address*)

• Problem B: Usability
  • We are bad at remembering addresses
  • Humans want names.

*slightly modified
Solving Problem A (Interopability)

- Add Identification of the Ledger instance
- Creates unique, and resolvable addresses
  - „Bitcoin“: 3E53XjqK4Cxt71BGeT2VhpcotV8LZ853C8
- Side problem: Ledger instance identification must be unique
  - Ensure that each Ledger „name“ is allocated just once
Background (2) – Decentralized Identifiers*

- Work of the W3C Credentials Community Group (soon to be „upgraded“ to a Working Group)
- URI-Scheme „did“ (Provisional Registration)
- Hierachical Scheme:

  `<scheme>:[<method>:<method-specific id>`
  `did:btrc:xzuc-wzcq-qppq-qupuzs8`

- Bingo! Solves our „Problem A“

*https://w3c-ccg.github.io/did-spec/*
Solving Problem B (Usability)

• Connect the unreadable addresses to a name!
• But: Which names, which technology?
• Globally unique, globally resolvable.
  • (Shhh, ... admitted, i’m a DNS person)

„Let’s put it into the DNS!“
Detour: Blockchain Namespaces

• The rise of „On Chain“ Naming Schemes
• Surprise: Syntax typically follows the DNS
  • Habit? Lack of creativity?
  • Or user adoption concerns? ;)
• Pioneer: Ethereum Name Service (ENS) under „.eth“
  • (namecoin — was a different, *important* step)
  • EOS, NNS, IOV, …
• But none of these name spaces are usable from the global DNS
  • Sometimes, they even collide with identical DNS spaces
  • Collisions create confusion, and defer the Interopability properties!
The "DNS Camel"

- New DNS work
- (Part of) the DNS community
- The poor overloaded DNS camel

Photo: Felice Beato on the Nile Expedition to relieve Khartoum, ca. 1884
• **RRType + Owner Name:** RFC 7553 – URI RRTyp
• **Email to DID:** RFC 7929 – DANE for OpenPGP
• **Service Parameter:** Existing IANA-Registry*
  • Allocation of „_did“ does not perfectly fit the Registry Policy
  • Ongoing discussions..

*https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
Running Code

- uniresolver.io
Next steps?

• What do dinrg members think? Is that useful?

• If you want that idea to proceed, please consider getting involved in dnsops discussions...

Thanks for listening!
alexander.mayrhofer@nic.at