Current State of DIDs

Markus Sabadello
Danube Tech, Decentralized Identity Foundation,
Sovrin Foundation, W3C CCG, OASIS XDI TC

https://danubetech.com/

TIIME – Vienna, 18th February 2019

DIF

DANUBE TECH GMBH

URNs (Uniform Resource Names, RFC 8141)

DIDs

The four core properties of a DID

1. **A permanent (persistent) identifier**

   It never needs to change

2. **A resolvable identifier**

   You can look it up to discover metadata

3. **A cryptographically-verifiable identifier**

   You can prove control using cryptography

4. **A decentralized identifier**

   No centralized registration authority is required

A DID Method...

Defines how to perform the **four CRUD operations** on a DID

1. **Create:** How to generate a new DID
2. **Read:** How to resolve a DID into a DID document
3. **Update:** How to write a new version of a DID document
4. **De-activate:** How to revoke (terminate) a DID so it no longer functions

A DID Document...

Contains metadata for describing and interacting with the DID subject (the entity identified by the DID)

1. **Public keys** or other cryptographic proof material
2. **Service endpoints** for engaging in trusted interactions
3. **Authentication mechanisms** for proving control of the DID
4. **Other metadata**

DID Resolution...

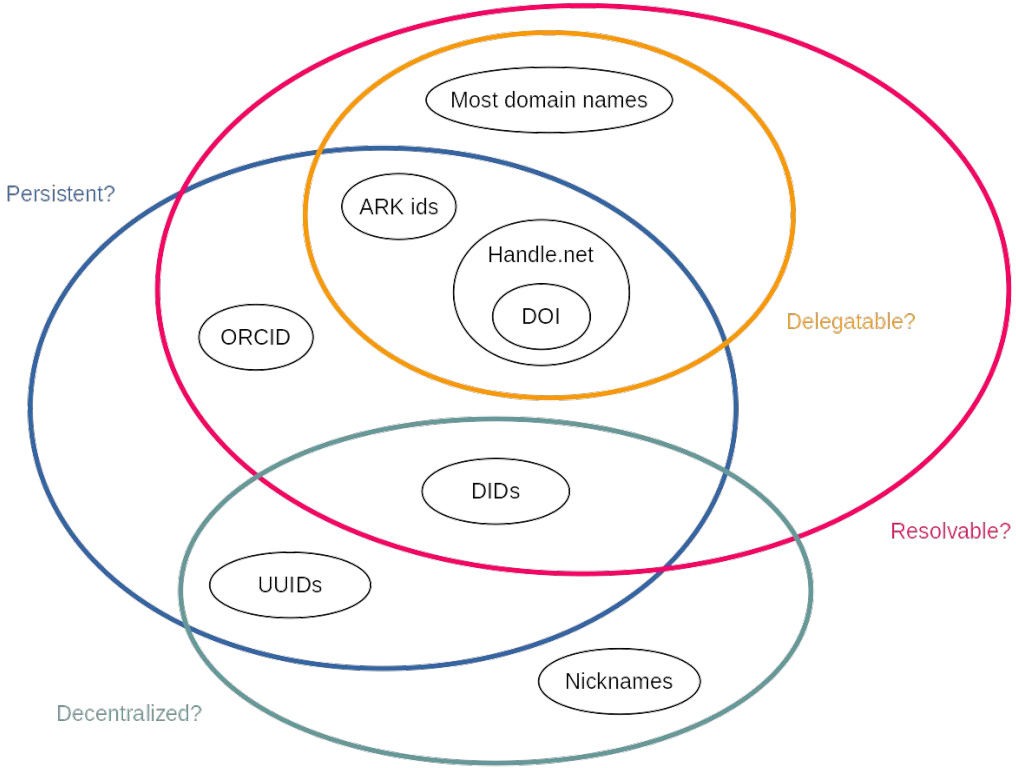
Is the process of using the DID to look up and retrieve a copy of the DID document

- How this is done depends on the DID method
  - Defined by the Read operation
- Different DID methods do this in different ways
- **DID Resolution** is a separate specification
  - **Not in scope** for the W3C DID Working Group

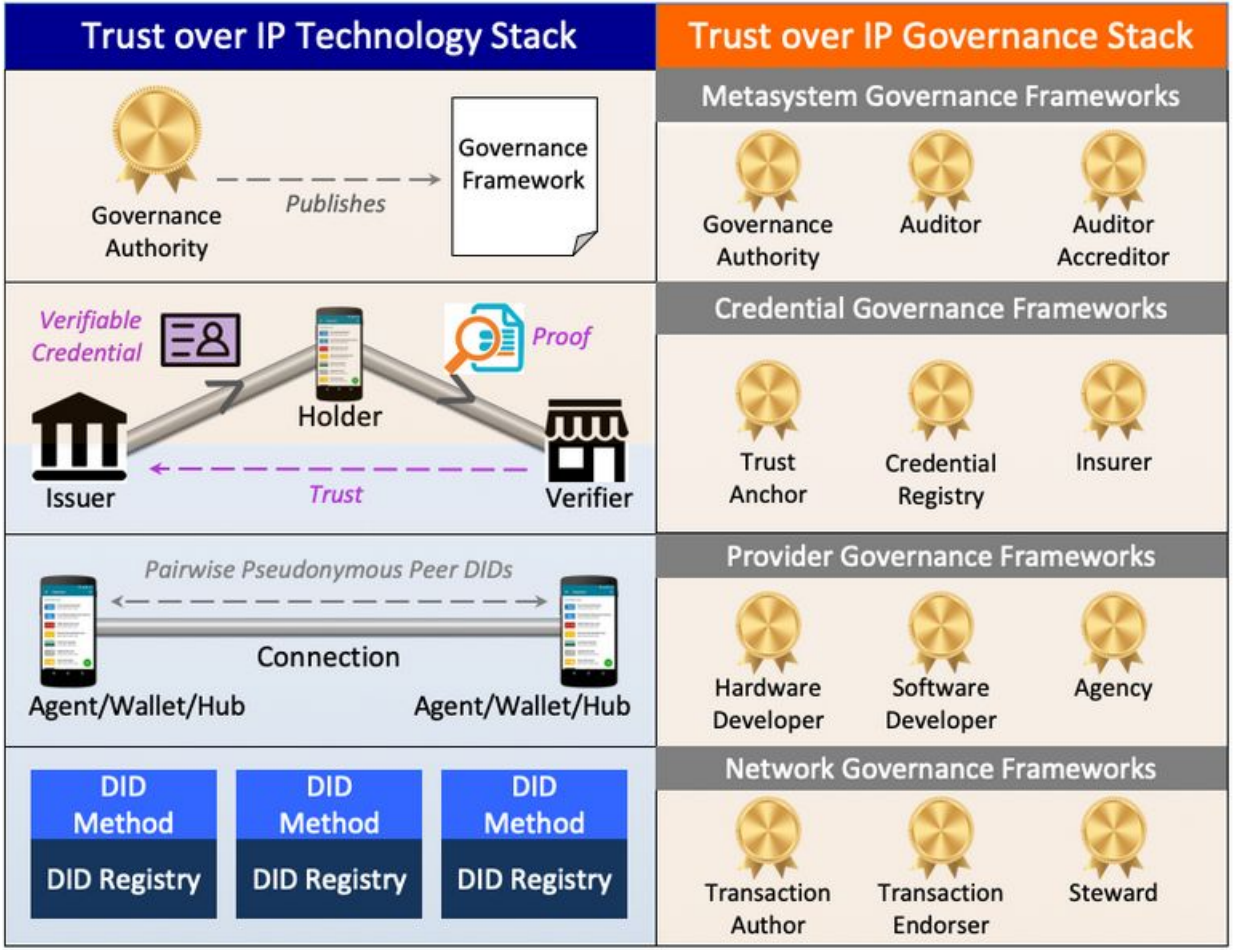
Comparing DIDs with Domain Names

Decentralized Identifiers (DIDs)	Domain Names
Globally unique	Globally unique
Persistent	Reassignable
Machine-friendly identifiers (i.e., long character strings based on random numbers / cryptography)	Human-readable names
Resolvable using different mechanisms defined by the applicable DID method	Resolvable using the standard DNS protocol
Associated data is expressed in DID documents	Associated data is expressed in DNS zone files
Fully decentralized namespaces without delegation	Hierarchical, delegatable namespaces based on centralized root registries for top-level domain names (TLDs)
Cryptographically-verifiable	Verifiable using DNS security extensions (DNSSEC)
Fully under the control of the DID controller	Ultimately controlled by ICANN and the registry operator for each DNS TLD

Comparison with other persistent identifiers



- DID Auth
- OIDC SIOP
- Verifiable Credentials
- DIDComm
- Agents
- Identity Hubs
- Encrypted Data Vaults
- ...



Amsterdam F2F Topics

- Major technical topics:
  - DID Document representations
  - Extensibility and interoperability
  - Metadata
  - Matrix parameters
- Additional topics:
  - Security, IoT, spec structure, rubric, use cases
  - Overlap with DID Resolution

Thank you

Markus Sabadello

Danube Tech
https://danubetech.com/
markus@danubetech.com

W3C DID WG:
https://www.w3.org/2019/did-wg/

DANUBE TECH GMBH