Decentralized IDentifiers (DIDs)

Markus Sabadello, M.Sc., M.A.
Danube Tech, Sovrin Foundation, OASIS XDI TC

https://danubetech.com/

W3C Workshop on Privacy and Linked Data,
Vienna, 17th April 2018
Intro: Self-Sovereign Identity

- Emerging paradigm: “Self-Sovereign Identity”

  “The central problem of the future is, how do we return control of our identities to the people themselves?”
  - Edward Snowden

  “DLT is generally well-suited to serve as the underlying technology for SSI because it offers a way to create a single source of identity that can be trusted by everyone, that is completely portable, but that no one entity owns or controls.”

- Combine digital human rights with industrial use of personal data.

2 W3C Workshop 2018-04-17
Decentralized IDentifiers (DIDs)

- Developed at Rebooting-the-Web-of-Trust workshop and W3C Credentials CG
- Persistent, dereference-able, cryptographically verifiable identifiers
- Registered in a blockchain or other decentralized network
- **did:sov:**3k9dg356wdcj5gf2k9bw8kfg7a
- Modular specification using “methods”:
  - **did:sov**, **did:btcr**, **did:v1**, **did:uport**, ...
- Can be pairwise unique for each relationship
- Resolution: DID → DID Document
  - Set of public keys
  - Set of service endpoints

<table>
<thead>
<tr>
<th>Method</th>
<th>DID Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sovrin</td>
<td>did:sov:</td>
</tr>
<tr>
<td>Bitcoin</td>
<td>did:btcr:</td>
</tr>
<tr>
<td>uPort</td>
<td>did:uport:</td>
</tr>
<tr>
<td>VeresOne</td>
<td>did:v1:</td>
</tr>
<tr>
<td>IPFS</td>
<td>did:ipid:</td>
</tr>
<tr>
<td>IPDB</td>
<td>did:ipdb:</td>
</tr>
<tr>
<td>Blockstack</td>
<td>did:stack</td>
</tr>
</tbody>
</table>
Decentralized IDentifiers (DIDs)

Example DID Document:

```json
{"@context": "https://w3id.org/did/v1",
"id": "did:btcr:xkrn-xzcr-qqlv-j6sl",
"service": [
  {
    "type": "agent",
  },
  {
    "type": "xdi",
    "serviceEndpoint": "https://xdi03-at.danubeclouds.com/cl/+!:did:btcr:xkrn-xzcr-qqlv-j6sl"
  }
],
"authentication": {
  "type": "EdDsaSASignatureAuthentication2018",
  "publicKey": [
    "did:btcr:xkrn-xzcr-qqlv-j6sl#key-1"
  ]
},
"publicKey": [
  {
    "id": "did:btcr:xkrn-xzcr-qqlv-j6sl",
    "type": "Secp256k1VerificationKey2018",
    "publicKeyHex": "024a63c4362772b0fafa5c51ac02470dae3f8da8a05d90bae9e1ef3f5243180120dd"
  }
]
}``
Decentralized IDentifiers (DIDs)

- Decentralized Identity Foundation:
  - https://identity.foundation/
- Universal Resolver / Universal Registrar
  - https://uniresolver.io/
- DPKI: Decentralized Public Key Infrastructure
- DKMS: Decentralized Key Management System
- Verifiable Credentials: Cryptographically verifiable statements
- DID Auth: Authentication, Single-Sign-On
- DID Names (BNS, ENS, ...), e.g. markus.id
Thank You

- https://danubetech.com/
- markus@danubetech.com
Intro: Self-Sovereign Identity

Definition:
“Lifetime portable identity for any person, organization, or thing that does not depend on any centralized authority and can never be taken away.”

Properties:
- Control
- Consent
- Contextual
- No central authority
- No intermediaries
- Minimal disclosure
- Choice of persistence
- Portable
- Inter-operable
- Technology pluralistic
Verifiable Credentials

- Verifiable Claims W3C WG (includes Linked Data Signatures)
- Credentials W3C CG and Digital Verification W3C CG
- Semantic data that is “attested” instead of “self-asserted”
- Cryptographically verifiable statements of an entity (“Issuer”, “Claimant”) about another entity (“Subject”, “Holder”), e.g.:  
  - Post office says: “Ms. Voshmgir has an address in Berlin.”
  - University says: “Mr. Sabadello has a computer science degree.”
  - Training Institution says: “Mr. Fölser is a certified aircraft technician.”

- Based on RDF data model and JSON-LD format, using DIDs or other URIs.
- Basis for “trust” and “reputation” in combination with a trust framework.
Verifiable Credentials

Example:

```json
{
   "@context": "https://w3id.org/security/v1",
   "id": "http://example.gov/credentials/3732",
   "type": ["Credential", "ProofOfAgeCredential"],
   "issuer": "https://dmv.example.gov",
   "issued": "2017-01-01",
   "claim": {
      "id": "did:sov:ebfeb1f712ebe6f1c276e12ec21",
      "ageOver": 21
   },
   "signature": {
      "type": "LinkedDataSignature2015",
      "created": "2016-06-18T21:19:10Z",
      "creator": "https://example.com/jdoe/keys/1",
      "domain": "json-ld.org",
      "nonce": "598c63d6",
      "signatureValue": "BavEll0/I1zpYw8Xi1bgVg/sCneO4Jugez8RWd/+ MCRvjo0bDoe4SsKjCoKvKioCGDvCk4Krgi6Z1n0UfqzxBfmatCuFibc1wps PRd+wGusvPTLzvMlwMhwYmfIFpbBu9S501+rSLHIEuujM/+PXy9Cky6Ed +W3JT24="
   }
}
```
Intro: Digital Identity

  - “The Internet was built without an Identity layer"

- Evolution:
  - Username+Password
  - Centralized: MS Passport/365, Login with Facebook, Google, Twitter
  - Enterprise/Government Identity Federation: SAML
  - User-Centric Identity: Eclipse Higgins, OpenID, Cardspace, OAuth, UMA
  - Federated Social Web: Diaspora, OStatus, IndieWeb
  - Personal Data Stores: Personal.com, MyDex, Azigo
  - Personal Clouds/PIMS: Meeco, CozyCloud, Digi.Me, Respect Network
  - Decentralization: Unhosted, Webfinger, WebID/Solid, XDI, FreedomBox
  - First-Party Terms, Consent Receipts, Link Contracts, DNT
  - Blockchain Identity: Namecoin, Blockstack, uPort, Sovrin, Jolocom, DIDs
## Blockchain Characteristics

### Who can operate a node?

<table>
<thead>
<tr>
<th>Public</th>
<th>Permissionless</th>
<th>Permissioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin</td>
<td>Ethereum</td>
<td>Sovrin</td>
</tr>
<tr>
<td>Ethereum</td>
<td>Veres One</td>
<td>IPDB</td>
</tr>
<tr>
<td>Veres One</td>
<td>IOTA</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Private</th>
<th>Permissionless</th>
<th>Permissioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hyperledger Sawtooth*</td>
<td></td>
<td>Hyperledger (Fabric, Sawtooth, Iroha)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R3 Corda</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CU Ledger</td>
</tr>
</tbody>
</table>

* in permissionless mode
Sovrin / Indy

- https://sovrin.org/
- Sovrin Foundation – Board of Trustees, Stewards, Technical Governance Board
- “Indy” = Open-source project at Hyperledger
- “Sovrin” = Public, permissioned deployment of Indy nodes
- Registration of DIDs and DID Documents
- Sovrin Trust Framework
- 24 Stewards in 12 countries
- Indy Nodes, Agents & Clients
Example Components

“On-chain” vs. “Off-chain”
Ledger/Agent Architecture

- **Identity Owner Layer**
  - Individuals

- **Edge Layer**
  - Edge Agents
  - Edge Wallets

- **Cloud Layer**
  - Cloud Agents
  - Cloud Wallets

- **Blockchain/DLT Layer**

Roles:
- Companies
- Public Institutions
- Things
Danube Tech GmbH

- https://danubetech.com/
- Founded 2015 in Vienna
- Working on core Sovrin and XDI infrastructure
- Strong international network
- “Founding Steward” at Sovrin Provisional Network
- “Founding Member” at Decentralized Identity Foundation
- “Founding Partner” at Respect Network
- Member of Personal Data Ecosystem Consortium
- Best of 10 at SBA “Security Rockstars” Competition
- Best of 15 at “Austria’s Next Top Start Up 2016”
- Selected for “Pioneers500” in 2016 und 2017
- Selected for “Netidee” (ISPA) Förderaktion in 2017
XDI

- “eXtensible Data Interchange”
- Protocol for data sharing and messaging
- Specifically designed for decentralized digital identity
- Vision: Global graph of personal and organizational data.
- Extension of the RDF graph model.
- Built-in support for “verifiable claims”, “connection requests”, “connection offers”, “link contracts”, “consent receipts”.
- Concept of “connectors” (aka “gateways”, “plugins”)
- Developed at OASIS XDI Technical Committee.
- 3rd generation, previously XRI/XDI.
Do you need a blockchain?

1. Do you need a database?
   - No: You don't need a blockchain
   - Yes: Do many people need to write to it?

2. Do many people need to write to it?
   - No: You don't need a blockchain
   - Yes: Do those people trust each other?

3. Do those people trust each other?
   - No: You don't need a blockchain
   - Yes: Do they have one person in common they trust?

4. Do they have one person in common they trust?
   - No: You need a blockchain
   - Yes: You don't need a blockchain

2018-04-17