Hyperledger Vienna #6: Identity for All

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

https://danubetech.com/

Hyperledger Vienna #6: Identity for All
Hyperledger Vienna

Tuesday, October 16, 2018
6:00 PM to 9:00 PM

Attend

nic.at Vienna Office
Karlsplatz 1, A-1010
right staircase, 3rd floor
Vienna

DIF

DANUBE TECH GMBH

"Missing Identity Layer"

DANUBE TECH GMBH

"Control, Consent, Context, Persistence, Portability, Pluralism"

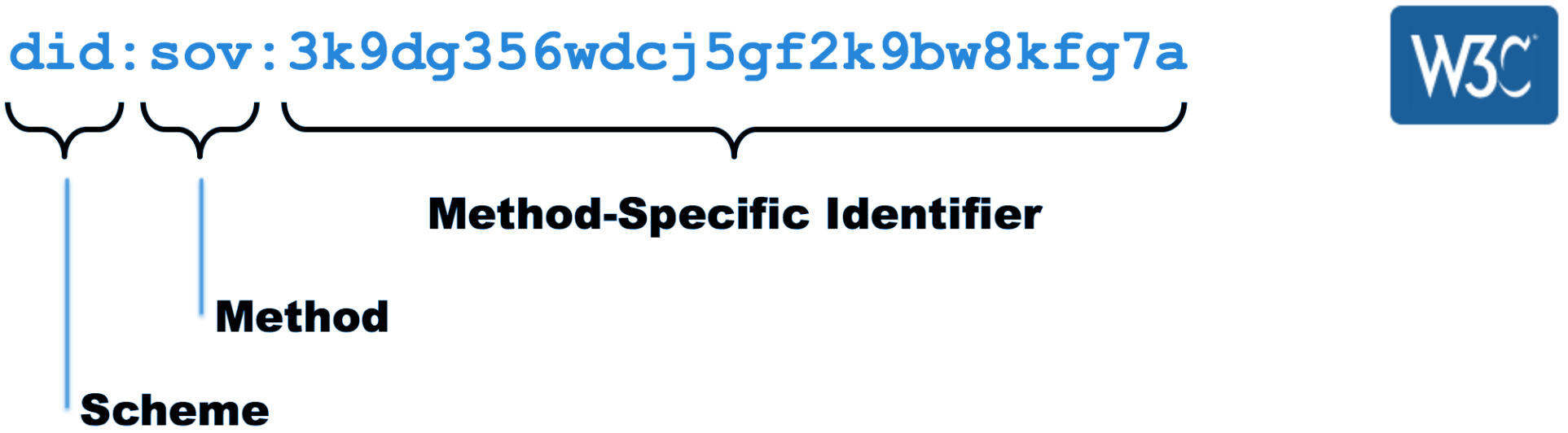
DANUBE TECH GMBH

Decentralized Identifiers (DIDs)

DANUBE TECH GMBH

Decentralized Identifiers (DIDs)

- Self-sovereign identifiers for individuals, organizations, things.
- Decentralized, persistent, cryptographically verifiable, dereference-able identifiers.
- Registered in blockchain or other decentralized network (ledger-agnostic).
- Created and managed via wallet application.



DID Document

- Registered in a blockchain or other decentralized network, or off-ledger
- Ledger-agnostic
- Resolution: DID → DID Document
  - Set of public keys
  - Set of service endpoints
  - Timestamps, proofs
  - Other identifier metadata


```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:sov:WRfXPg8dantKVubE3HX8pw",
  "service": {
    "type": "hub",
    "serviceEndpoint": "https://azure.microsoft.com/dif/hub/
did:sov:WRfXPg8dantKVubE3HX8pw"
  },
  "publicKey": [
    {
      "id": "did:sov:WRfXPg8dantKVubE3HX8pw#key-1",
      "type": "Ed25519VerificationKey2018",
      "publicKeyBase58":
"H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDmqPV"
    }
  ],
  "authentication": {
    "type": "Ed25519SignatureAuthentication2018",
    "publicKey": [
      "did:sov:WRfXPg8dantKVubE3HX8pw#key-1"
    ]
  }
}
```


DANUBE TECH GMBH

DID Methods

- Different DID “methods”:
- **`did:sov`**, **`did:btcr`**, **`did:v1`**, **`did:uport`**, …
- All methods need:
  - A DID method specification (W3C)
  - An implementation of a “resolver”
- Define method-specific syntax
- Define CRUD for DIDs:
  - Create, Read (Resolve), Update, Delete (Revoke)

Method	DID Prefix
Sovrin	`did:sov:`
Veres One	`did:v1:`
uPort	`did:uport:`
Bitcoin	`did:btcr:`
Blockstack	`did:stack:`
ERC725	`did:erc725:`
IPFS	`did:ipid:`

DANUBE TECH GMBH

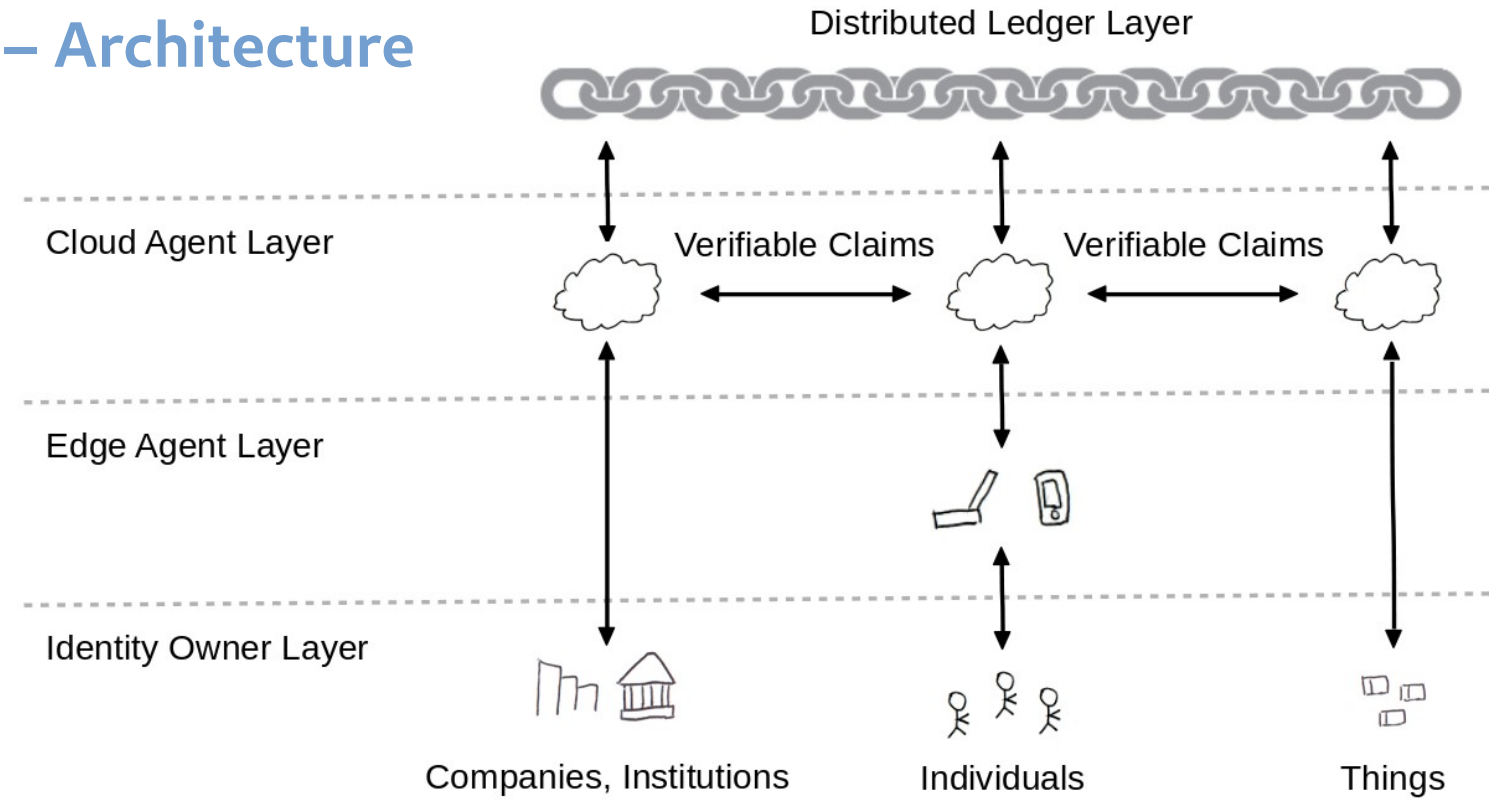
Hyperledger Indy and Sovrin

HYPERLEDGER
INDY

sovrin
identity for all

DANUBE
TECH GMBH

Hyperledger Indy – Architecture

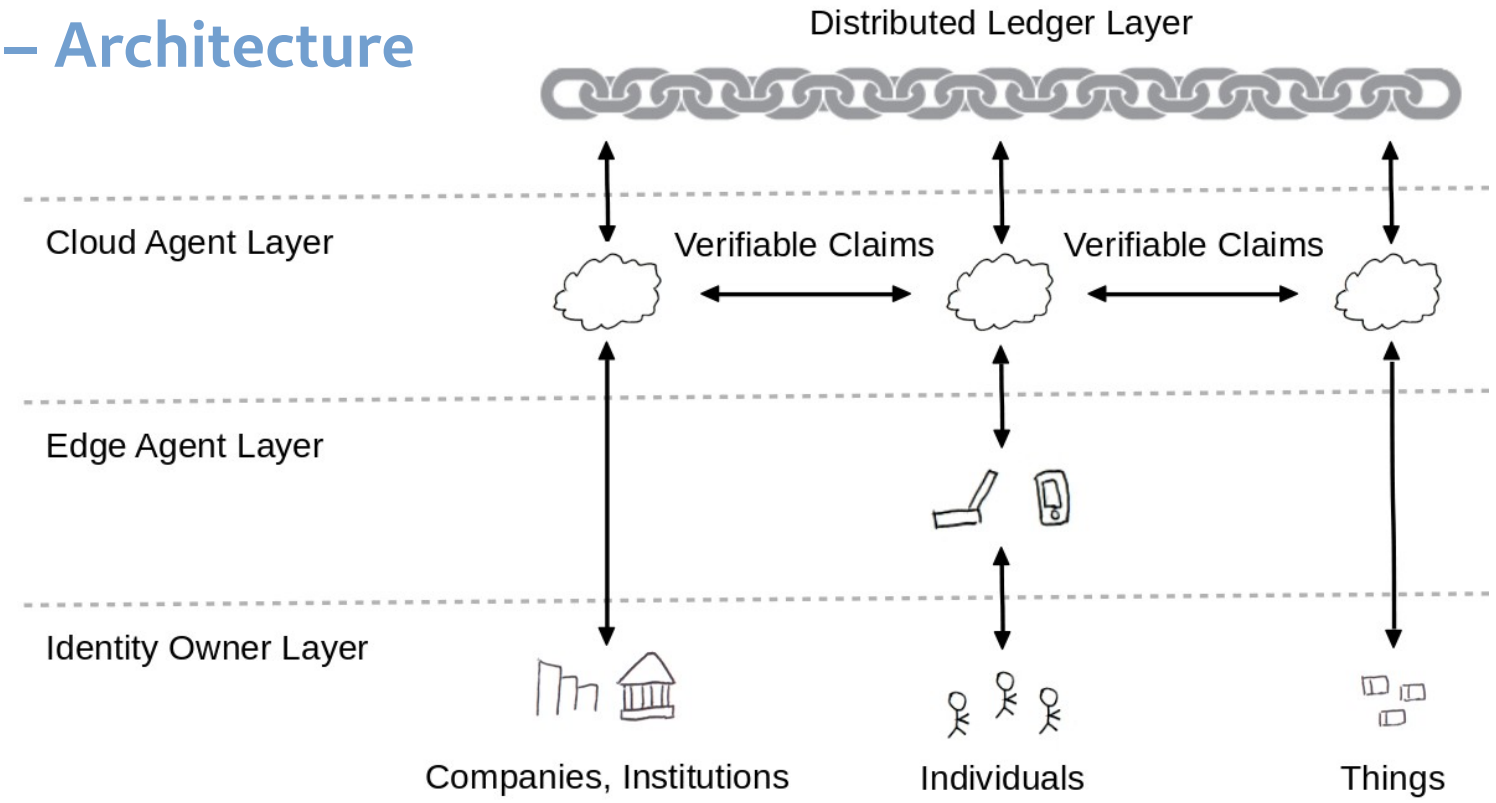


HYPERLEDGER INDY

DANUBE TECH GMBH

Hyperledger Indy – Architecture

- On-ledger:
  DIDs, Schemas,
  Revocation Lists
- Off-ledger:
  Credentials, Claims,
  Proofs, Messages



HYPERLEDGER INDY

DANUBE TECH GMBH

Hyperledger Indy

"Tools, libraries, and reusable components for providing digital identities rooted on blockchain or other distributed ledgers so that they are interoperable across administrative domains, applications, and any other silo."

indy-crypto	indy-plenum	indy-node	indy-agent	indy-sdk
Shared crypto library for CL and BLS signatures	Implementation of RBFT consensus protocol	Code to run validator and observer nodes	Provides control and storage for identity owners	SDK for ledger, credentials, and agent access

Includes wrappers and CLI

HYPERLEDGER INDY

DANUBE TECH GMBH

Indy SDK / CLI

- APIs:

  pool
  wallet
  did
  ledger
  anoncreds

```
Pool "stn" has been connected
pool(stn):indy> wallet open mywallet key
Enter value for key:

Wallet "mywallet" has been opened
pool(stn):wallet(mywallet):indy> did new
Did "HfEgjxf986KnSz9K3NcXCL" has been created with "~LdqGAnQzwyA7iDsTQ4XjZF" verkey
pool(stn):wallet(mywallet):indy> ledger nym did=HfEgjxf986KnSz9K3NcXCL verkey=~LdqGAnQzwyA7iDsTQ4XjZF
There is no active did
pool(stn):wallet(mywallet):indy> did list
+------------------------+-------------------------+----------+
| Did                    | Verkey                  | Metadata |
+------------------------+-------------------------+----------+
| 5Pr3DNAjv89syJadJpkiwV | ~4aSkMKFZHhmFfwepDuco2b | -        |
+------------------------+-------------------------+----------+
| HfEgjxf986KnSz9K3NcXCL | ~LdqGAnQzwyA7iDsTQ4XjZF | -        |
+------------------------+-------------------------+----------+
| WRfXPg8dantKVubE3HX8pw | ~P7F3BNs5VmQ6eVpwkNKJ5D | -        |
+------------------------+-------------------------+----------+
pool(stn):wallet(mywallet):indy> did use WRfXPg8dantKVubE3HX8pw
Did "WRfXPg8dantKVubE3HX8pw" has been set as active
pool(stn):wallet(mywallet):did(WRf...8pw):indy> ledger nym did=HfEgjxf986KnSz9K3NcXCL verkey=~LdqGAnQzwyA7iDsTQ4XjZF
Nym request has been sent to Ledger.
Metadata:
+------------------------+-----------------+---------------------+---------------------+
| From                   | Sequence Number | Request ID          | Transaction time    |
+------------------------+-----------------+---------------------+---------------------+
| WRfXPg8dantKVubE3HX8pw | 9445            | 1539674448774274857 | 2018-10-16 07:20:49 |
+------------------------+-----------------+---------------------+---------------------+
Data:
+------------------------+-------------------------+------+
| Did                    | Verkey                  | Role |
+------------------------+-------------------------+------+
| HfEgjxf986KnSz9K3NcXCL | ~LdqGAnQzwyA7iDsTQ4XjZF | -    |
+------------------------+-------------------------+------+
pool(stn):wallet(mywallet):did(WRf...8pw):indy>
```

HYPERLEDGER
INDY

DANUBE
TECH GMBH

Sovrin

- An instance of a Hyperledger Indy distributed ledger
- “Global public utility for identity”
- Permissioned (proof-of-authority)
- Non-profit Sovrin Foundation
- Sovrin Governance Framework

sovrin

identity for all

DANUBE TECH GMBH

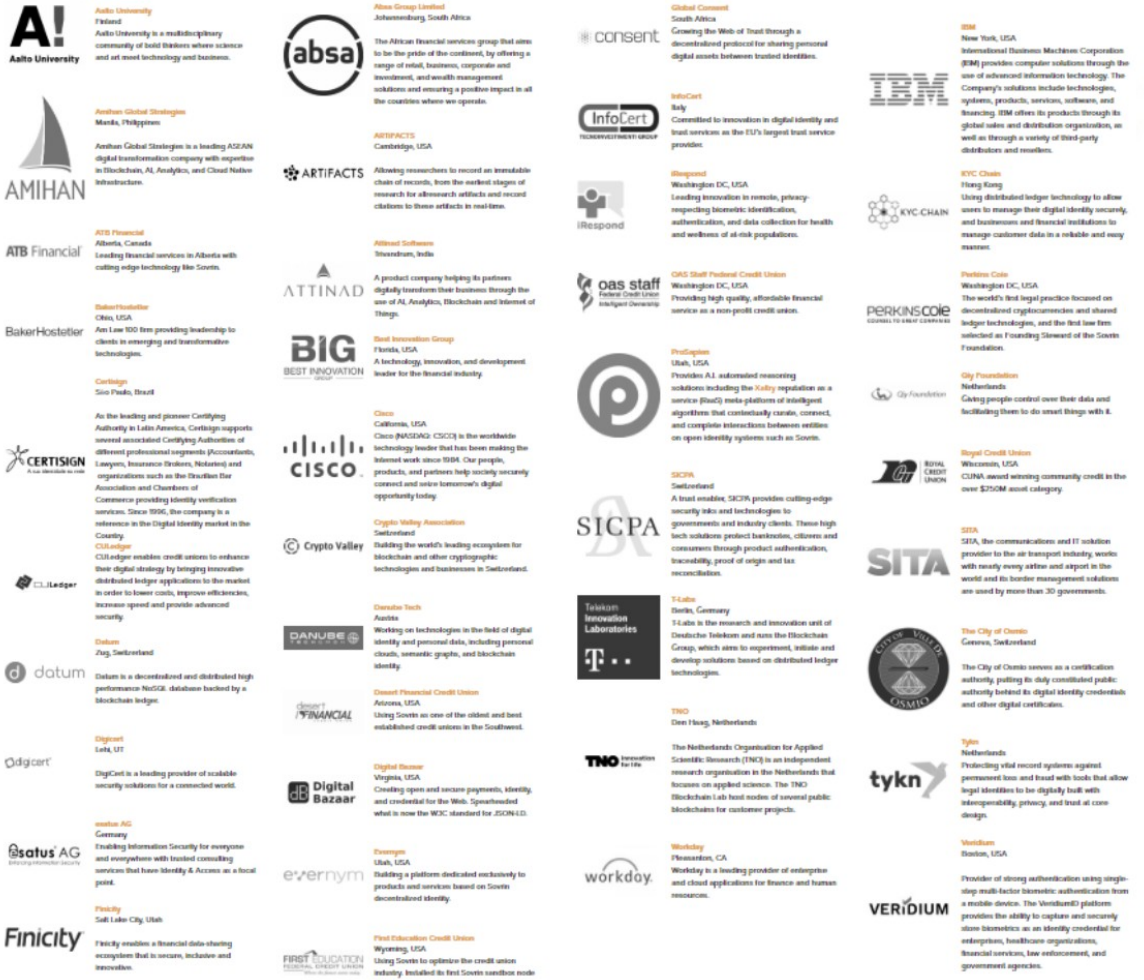
Sovrin

- About 40 “Stewards” who operate ledger nodes
- Financial institutions, certification authorities, tech companies, law firms, NGOs, universities, etc.
- Governed by Sovrin Foundation

Who operates the ledger nodes?

Who can use the ledger?

	Permissionless	Permissioned
Public	Bitcoin Ethereum	Sovrin
Private	Hyperledger Sawtooth* * in permissionless mode	Hyperledger (Fabric, Sawtooth, Iroha) R3 Corda CU Ledger



DANUBE TECH GMBH

Hyperledger Indy

- Chat:
  https://chat.hyperledger.org/channel/indy
- Mailing List:
  https://lists.hyperledger.org/g/indy
- Working Group Call: Thursday 8am PDT = 5pm CEST
  https://zoom.us/j/hyperledger-community
- Wiki:
  https://wiki.hyperledger.org/projects/indy
- Project Enhancement:
  https://github.com/hyperledger/indy-hipe

HYPERLEDGER
INDY

DANUBE
TECH GMBH

Thank You

- https://danubetech.com/
- markus@danubetech.com

DIF

DANUBE TECH GMBH

Extra Slides

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

UBS

"...we think self-sovereign [identity] solutions are likely to be the standard against which other platforms will need to be held."

PERKINSCOIE
COUNSEL TO GREAT COMPANIES

"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."

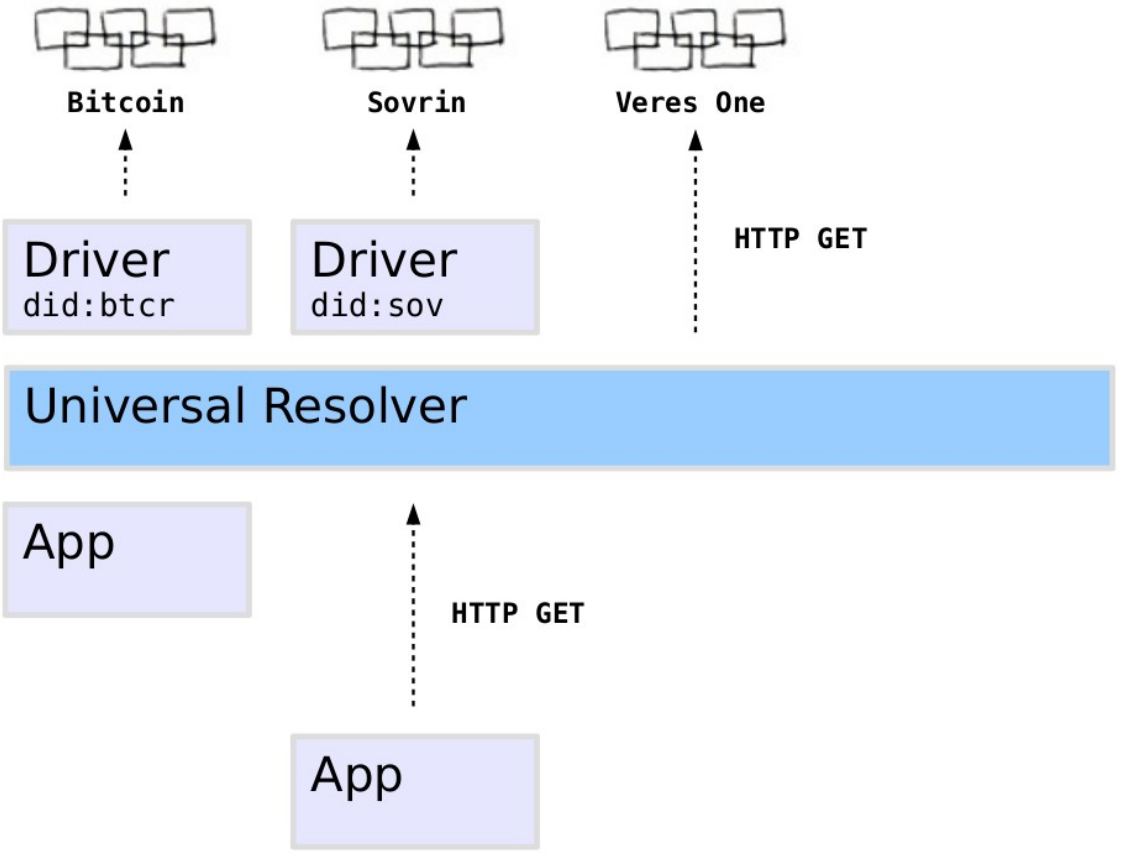
Craig Newmark
Founder, CraigsList

"I'd like to use [blockchain] for verifiable identity."

DANUBE TECH GMBH

DID Universal Resolver

- Looks up (“resolves”) DID to its DID Document.
- Provides a universal API that works with all DID methods.
- Uses a set of configurable “drivers” that know how to connect to the target system.
- Can return metadata about the resolution process.
- **https://uniresolver.io/**



DIF

DANUBE TECH GMBH

Proof-of-Concept: myIDsafe

myIDsafe

DANUBE TECH GMBH

Proof-of-Concept: myIDsafe

DANUBE TECH GMBH

Legal Developments

GDPR:

1) Access to identity data is only possible via individual's agent.
2) Consent is digitally signed and is visible to involved parties
3) Consent can always be revoked using agents, and connected companies are notified.
4) Agents enable data portability.
5) Off-ledger DIDs and ZKPs allow data minimization on the ledger.

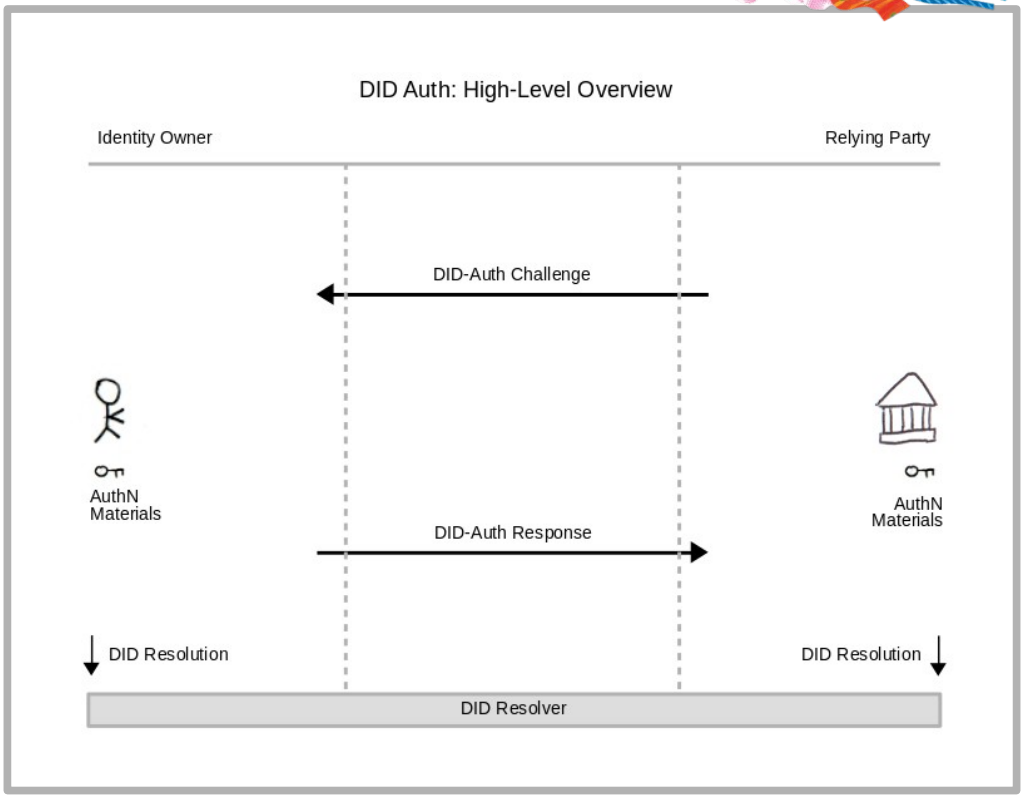
eIDAS

1) Qualified eID attribute can be "derived" to Verifiable Credentials.
2) Trust in state-verified identity is "imported" into SSI ecosystem.
3) Facilitates the Trust Framework and questions of liability.
4) Combine identity data from public sector, economy, and civil society.
5) Off-ledger DIDs and ZKPs allow data minimization on the ledger.

DANUBE TECH GMBH

DID Auth

- Identity owner interacts with a relying party.
- Prove control of a DID using a cryptographic challenge/response protocol.
- Prove that “I am me”.
- Different architectures and scenarios.



Introduction to DID Auth

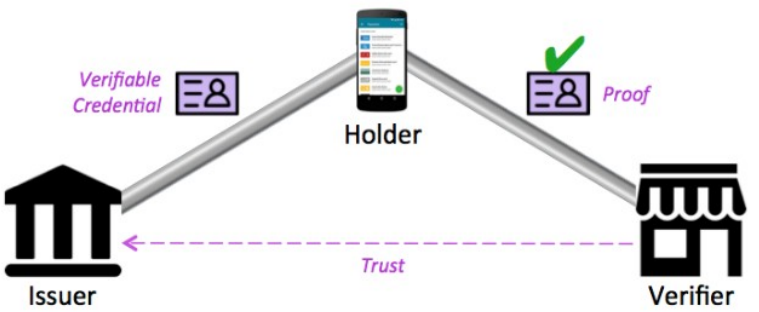
A White Paper from Rebooting the Web of Trust VI

by Markus Sabadello, Kyle Den Hartog, Christian Lundkvist, Cedric Franz, Alberto Elias, Andrew Hughes, John Jordan, and Dmitri Zagidulin

DANUBE TECH GMBH

Verifiable Credentials

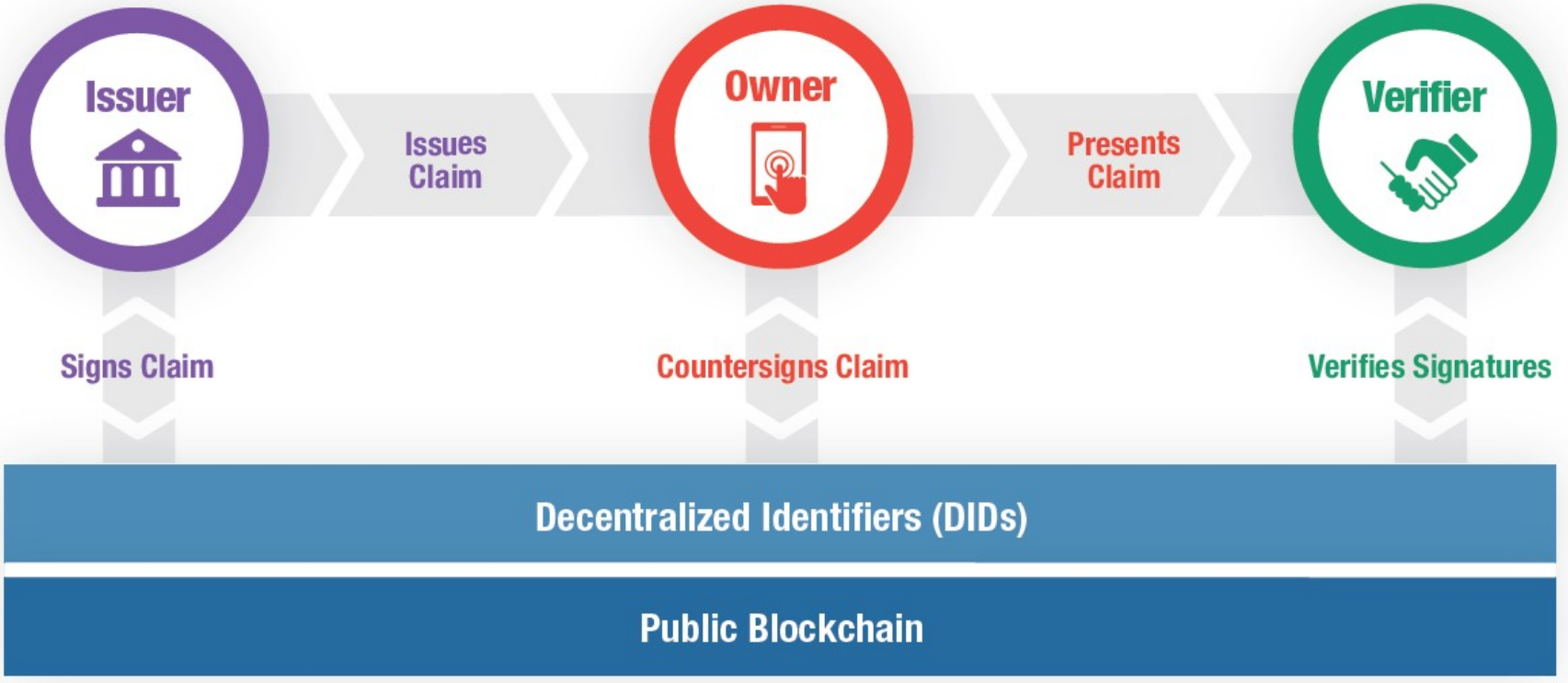
- Identity data, that is “attested” by a trusted party instead of “self-asserted”.
- Cryptographically verifiable.
- Semantic statements expressed in JSON-LD / RDF, e.g.:
  - Post attests: I live in 1170 Vienna.
  - University attests: I have a diploma in Computer Science.
  - Bank attests: My credit score is sufficient for a given transaction.
  - Government attests: My name and birthday are …



“Trust Framework”

DANUBE TECH GMBH

Verifiable Credentials



DANUBE TECH GMBH

Verifiable Credentials

- Example:


```
{
  "@context": "https://w3id.org/credentials/v1",
  "id": "did:sov:WRfXPg8dantKVubE3HX8pw/credentials/1",
  "type": ["Credential", "NameCredential"],
  "issuer": "did:sov:WRfXPg8dantKVubE3HX8pw",
  "issued": "2018-05-01",
  "claim": {
    "id": "did:btcr:x6lj-wzvr-qqrv-m80w",
    "name": "Markus Sabadello",
    "adresse": "..."
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2017-06-18T21:19:10Z",
    "creator": "did:sov:WRfXPg8dantKVubE3HX8pw#key-1",
    "nonce": "c0ae1c8e-c7e7-469f-b252-86e6a0e7387e",
    "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCneO4Jugez8RwDg/+
      MCRVpjOboDoe4SxxKjkCOvKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
      PRdW+gGsutPTLzvueMWmFhwYmfIFpbBu95t501+rSLHIEuujM/+PXr9Cky6Ed
      +W3JT24="
  }
}
```


DANUBE TECH GMBH

Verifiable Credentials

DKMS, DID Auth

Hubs, Agents, XDI

Yadis, XRI, XRD, XRDS, JRD, Webfinger

W3C Web Payments CG

OASIS XDI TC

DIDs: W3C Credentials CG
v0.10 Draft Community Report

DIDs: W3C DID WG
Charter now being written

Rebooting-the-Web-of-Trust
Internet Identity Workshop

DID registered
prov. URI scheme

DID method specs

W3C JSON-LD 1.1

W3C Cryptographic Suites

RFC 7517: JWK

DANUBE TECH GMBH