Decentralized Identifers (DIDs)

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

https://danubetech.com/

sec4dev – Vienna, 26th February 2019

DIF

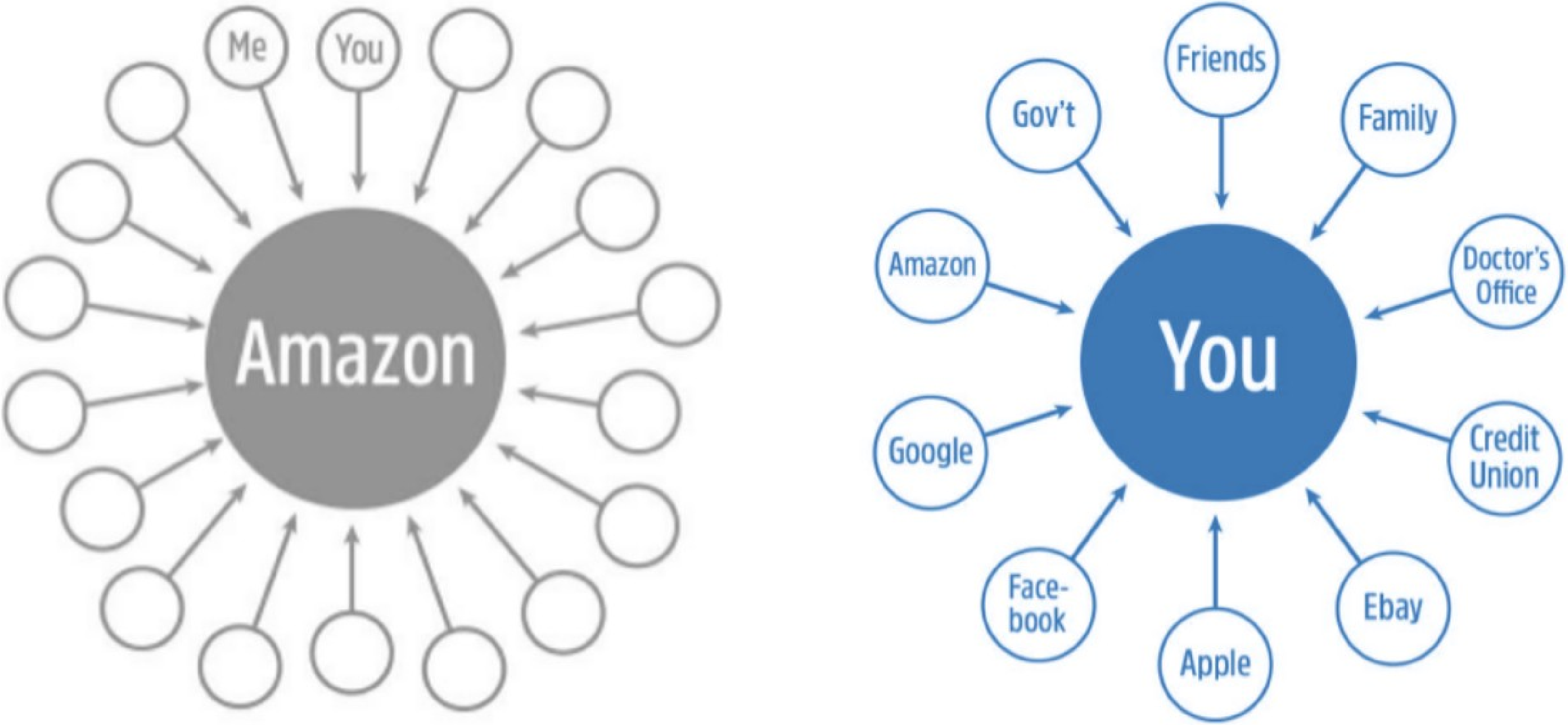
DANUBE
TECH GMBH

... so home values and rents will soar due to hedonistic wage rises ...
P. Steiner

"On the Internet, nobody knows you're a dog."

Digital Identity

Internet Identity Workshop



Self-Sovereign Identity

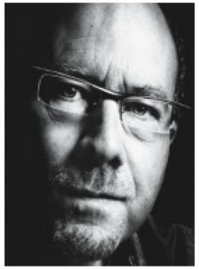
“The central problem of the future is, how do we return control of our identities to the people themselves?”
- Edward Snowden

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.”

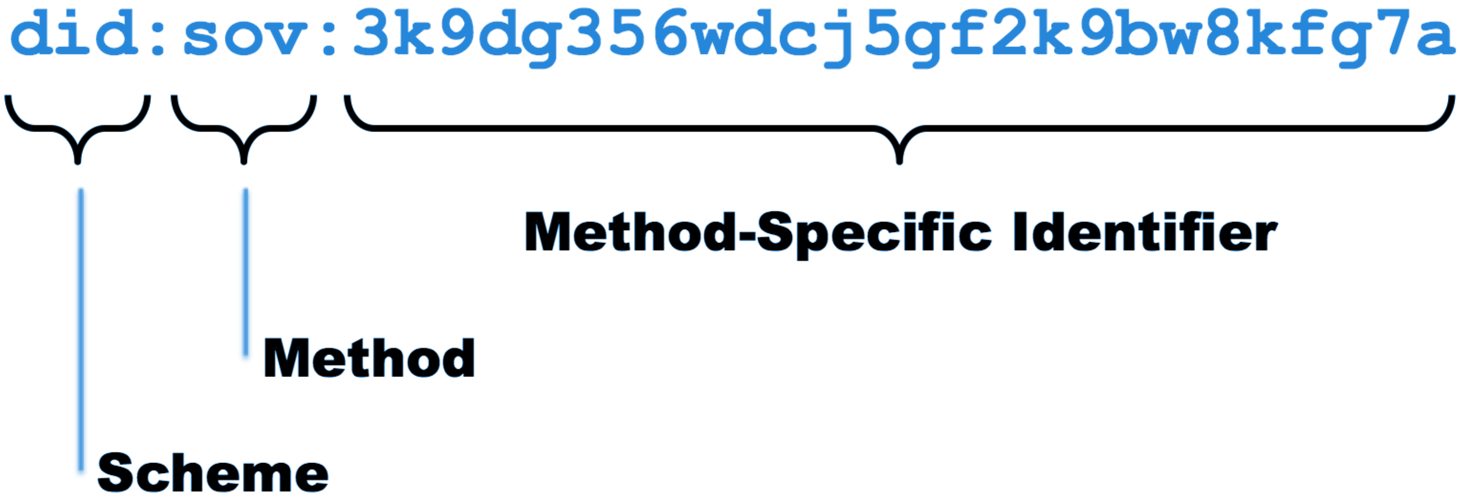


Craig Newmark
Founder, CraigsList

“I’d like to use [blockchain] for verifiable identity.”

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 by identity controller via wallet application.



did:sov:3k9dg356wdcj5gf2k9bw8kfg7a

Method-Specific Identifier

Method

Scheme

DID Methods

- Different DID “methods”:

```
did:sov:WRfXPg8dantKVubE3HX8pw
did:btcr:xz35-jzv2-qqs2-9wjt
did:v1:test:nym:3AEJTDMSxDDQpyUftjuoeZ2Bazp4Bswj1ce7FJGybCUu
did:uport:2omWsSGspY7zhxaG6uHyoGtcYxoGeeohQXz
did:erc725:ropsten:2F2B37C890824242Cb9B0FE5614fA2221B79901E
```

- DID methods need a method specification.
- Define method-specific syntax.
- Define method-specific CRUD operations:
  - 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:`

DID Resolution

- DID Resolution: DID → DID Document
  - Set of public keys
  - Set of service endpoints
  - Authentication methods
  - Timestamps, proofs
  - Other identifier metadata

- May be dynamically constructed rather than actually stored in this form.
- Can support resolution parameters.
- Can return resolution metadata.

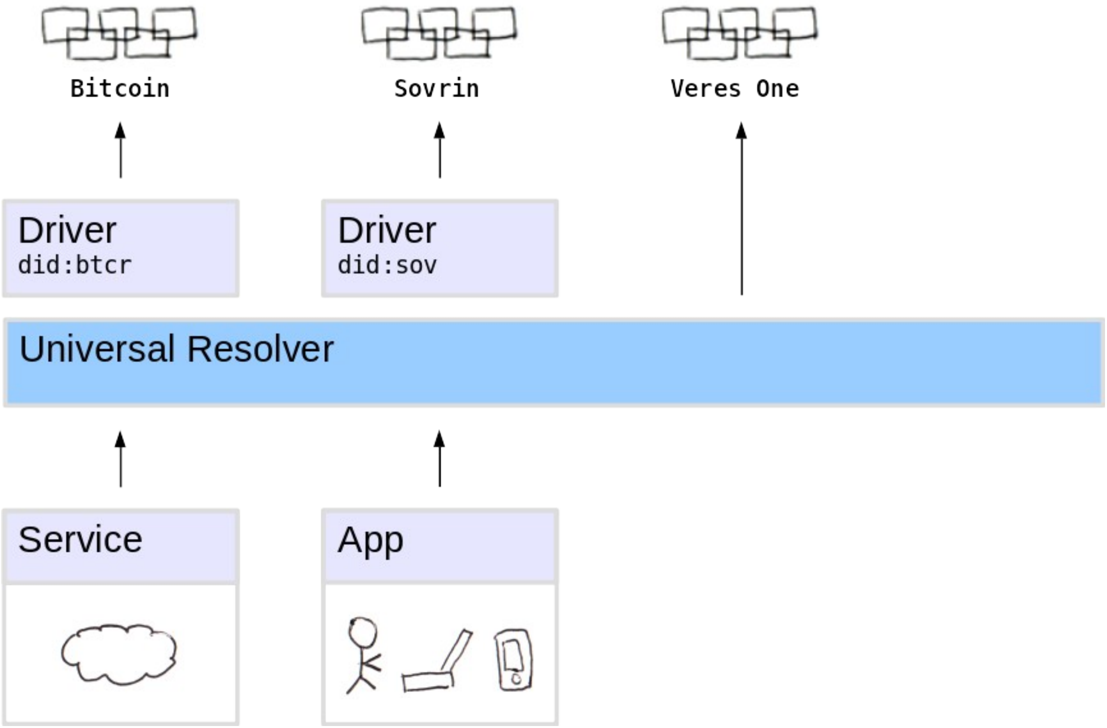
- Example DID Document:

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:sov:WRfXPg8dantKVubE3HX8pw",
  "publicKey": [
    {
      "id": "did:sov:WRfXPg8dantKVubE3HX8pw#key-1",
      "type": "Ed25519VerificationKey2018",
      "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDmqPV"
    }
  ],
  "service": {
    "type": "hub",
    "serviceEndpoint":
    "https://azure.microsoft.com/hub/did:sov:WRfXPg8dantKVubE3H"
  },
  "authentication": {
    "type": "Ed25519SignatureAuthentication2018",
    "publicKey": [
      "did:sov:WRfXPg8dantKVubE3HX8pw#key-1"
    ]
  }
}
```

DANUBE TECH GMBH

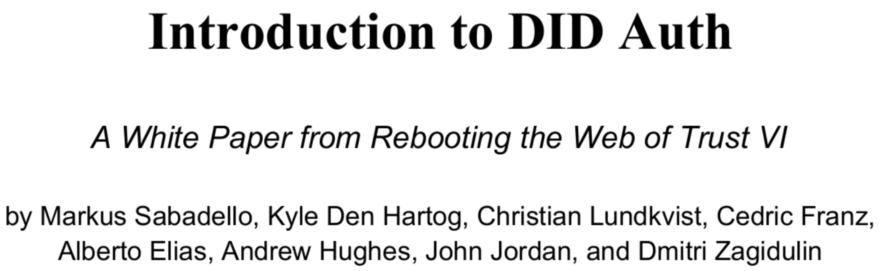
DID Universal Resolver

- 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.
- **https://uniresolver.io/**



DID Auth

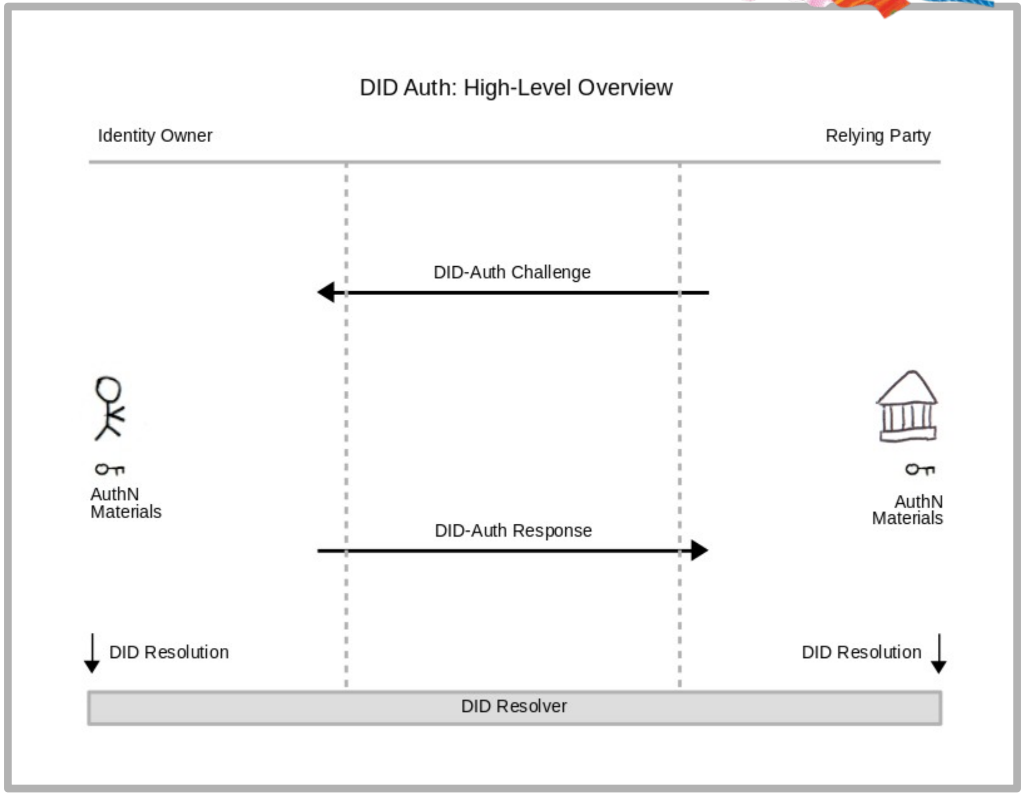
- Identity owner interacts with a relying party.
- Prove control of a DID using a cryptographic challenge/response protocol.
- Prove that “I am me”.
- Different architectures and scenarios.



Introduction to DID Auth

A White Paper from Rebooting the Web of Trust VI

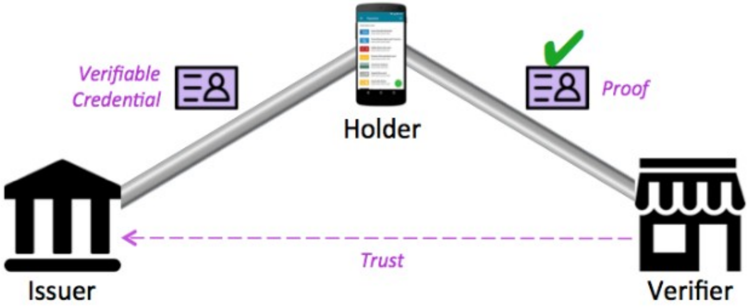
by Markus Sabadello, Kyle Den Hartog, Christian Lundkvist, Cedric Franz, Alberto Elias, Andrew Hughes, John Jordan, and Dmitri Zagidulin



DANUBE TECH GMBH

Verifiable Claims

- 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" for legal and business rules.

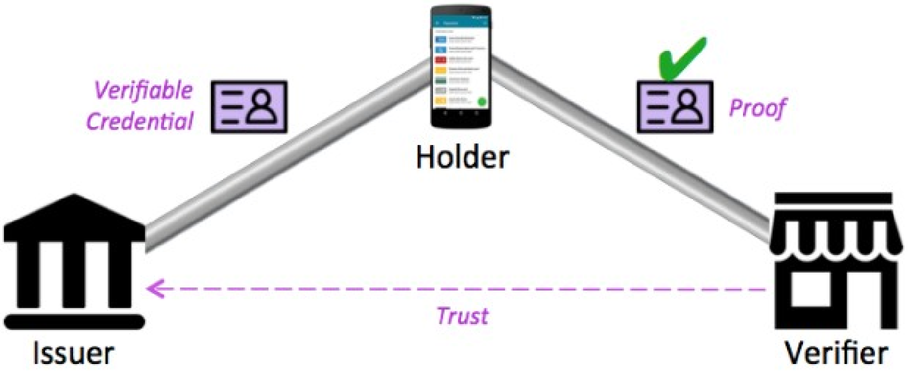


DANUBE TECH GMBH

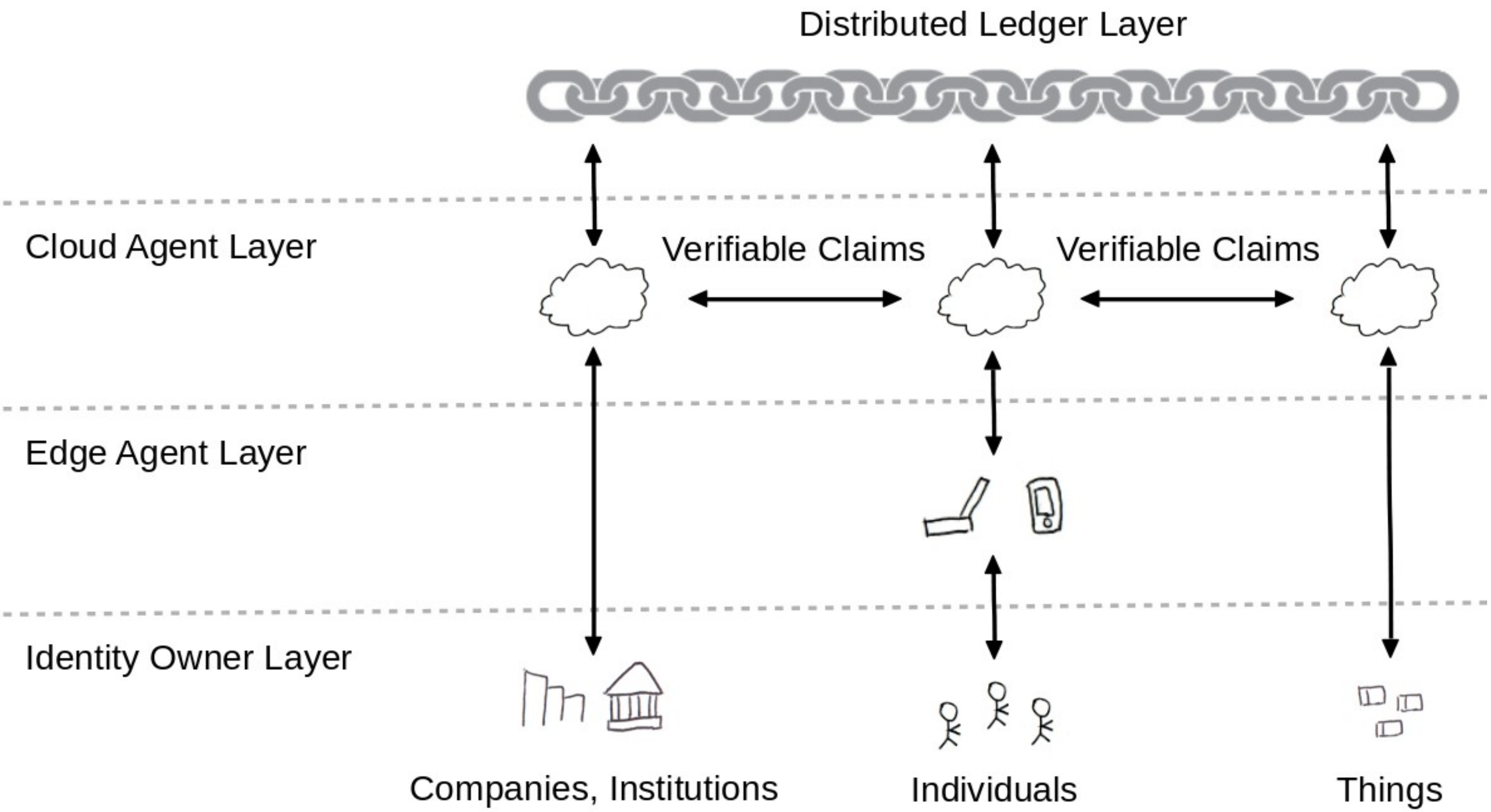
Verifiable Claims

- 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",
    "address": "..."
  },
  "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="
  }
}
```



Self-Sovereign Identity Technology



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
v0.11 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

Thank You

- **Internet Identity Workshop!** – April 30 2019 - May 2 2019, Mountain View, US
  - https://www.internetidentityworkshop.com/
- **W3C Credentials Community Group!**
  - https://w3c-ccg.github.io/
- **Decentralized Identity Foundation!**
  - https://identity.foundation/

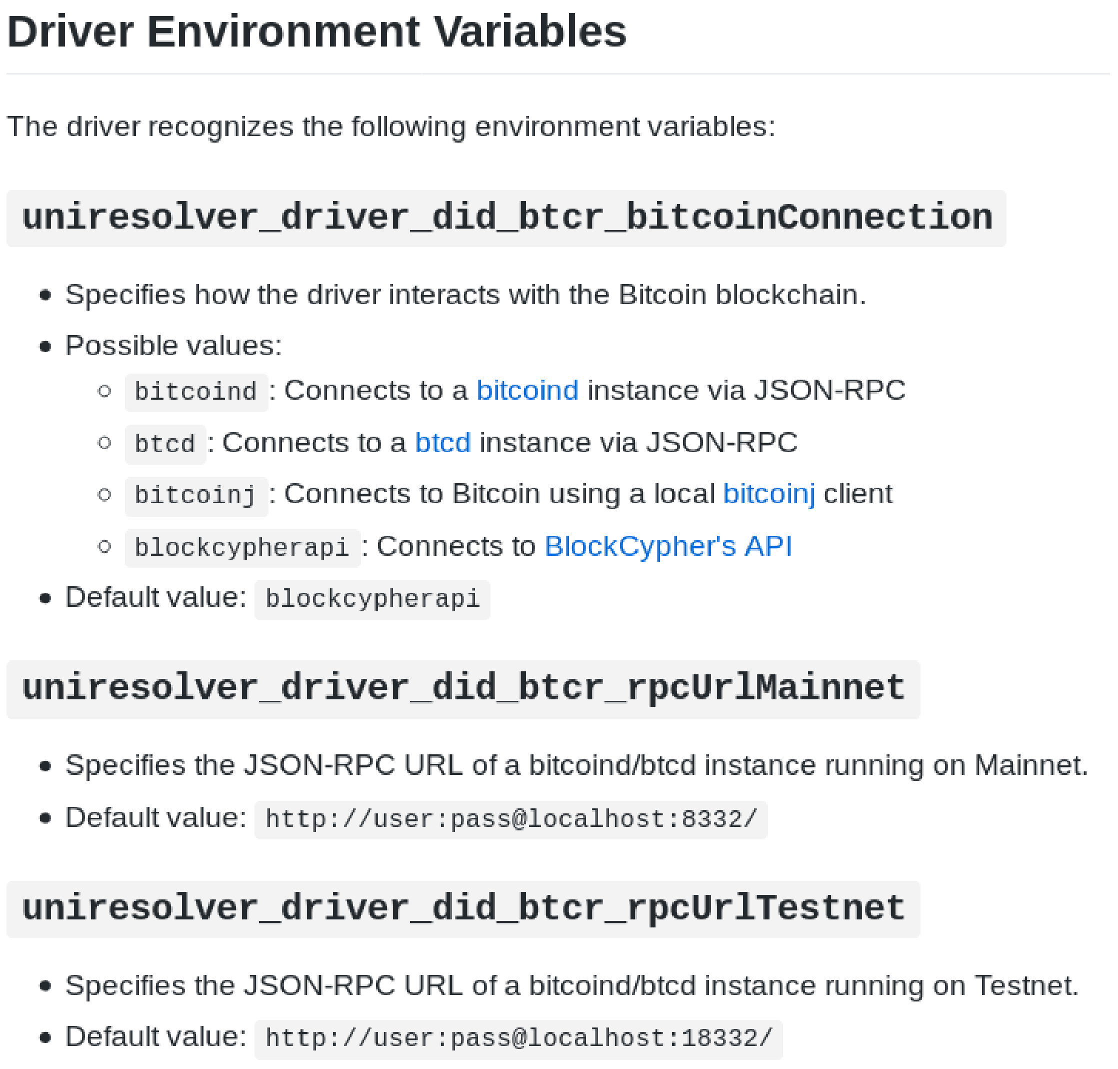
- https://danubetech.com/ – **markus@danubetech.com**

Extra Slides

DID Universal Resolver

- Example Driver Configuration:

```
{
  "pattern": "^(did:btcr:.+)$",
  "image": "universalresolver/driver-did-btcr",
  "tag": "latest",
  "testIdentifiers": [
    "did:btcr:xz35-jzv2-qqs2-9wjt",
    "did:btcr:x705-jzv2-qqaz-7vuz",
    "did:btcr:xkrn-xzcr-qqlv-j6sl"
  ],
  "env": {
    "uniresolver_driver_did_btcr_bitcoinConnection":
        "blockcypherapi",
    "uniresolver_driver_did_btcr_rpcUrlMainnet":
        "http://user:pass@localhost:8332/",
    "uniresolver_driver_did_btcr_rpcUrlTestnet":
        "http://user:pass@localhost:18332/"
  }
}
```



Driver Environment Variables

The driver recognizes the following environment variables:

`uniresolver_driver_did_btcr_bitcoinConnection`

- Specifies how the driver interacts with the Bitcoin blockchain.
- Possible values:
  - `bitcoind` : Connects to a bitcoind instance via JSON-RPC
  - `btcd` : Connects to a btcd instance via JSON-RPC
  - `bitcoinj` : Connects to Bitcoin using a local bitcoinj client
  - `blockcypherapi` : Connects to BlockCypher's API
- Default value: `blockcypherapi`

`uniresolver_driver_did_btcr_rpcUrlMainnet`

- Specifies the JSON-RPC URL of a bitcoind/btcd instance running on Mainnet.
- Default value: `http://user:pass@localhost:8332/`

`uniresolver_driver_did_btcr_rpcUrlTestnet`

- Specifies the JSON-RPC URL of a bitcoind/btcd instance running on Testnet.
- Default value: `http://user:pass@localhost:18332/`

DID Resolution: Input

- Additional input parameters:
  - Select specific resource in the DID Document by ID, e.g.

    `did:sov:WRfXPg8dantKVubE3HX8pw#key-1`
  - Select public key by type, e.g.

    `Ed25519VerificationKey2018`
  - Select authentication method by type, e.g.

    `Ed25519SignatureAuthentication2018`
  - Select service by type, e.g.

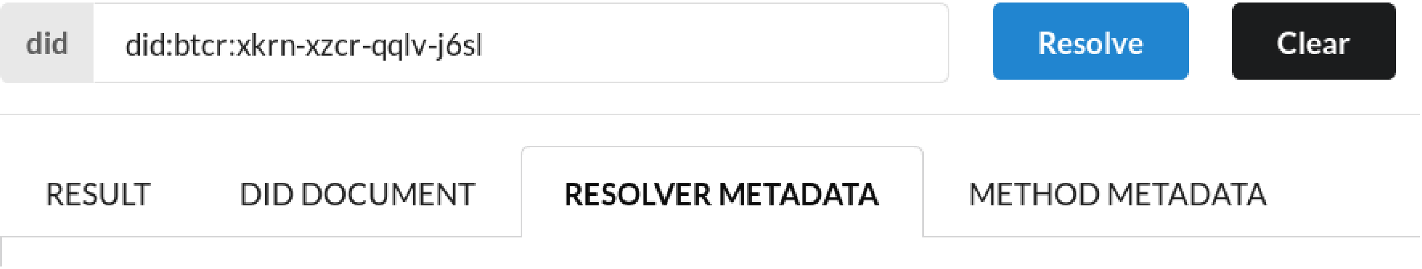
    `SocialWebInboxService`
  - Select service by name, e.g.

    `did:example:123456789abcdefghi;xdi`
  - Request specific version of DID Document, e.g. by version number, or by timestamp.
  - Request specific caching behavior, e.g. force fresh DID resolution.

DID Resolution: Output

- Resolver Metadata:
  - Which driver was used?
  - Duration of the resolution process?
  - Versioning information about the DID Document
  - Caching information about the DID Document

- Method Metadata:
  - Sovrin: State proofs from the ledger
  - Bitcoin: Was a full node used, or a external blockchain explorer?
  - Bitcoin: Transaction number and number of confirmations?
  - Bitcoin: Mainnet or Testnet?



did: did:btcr:xkrn-xzcr-qqlv-j6sl

DANUBE TECH GMBH

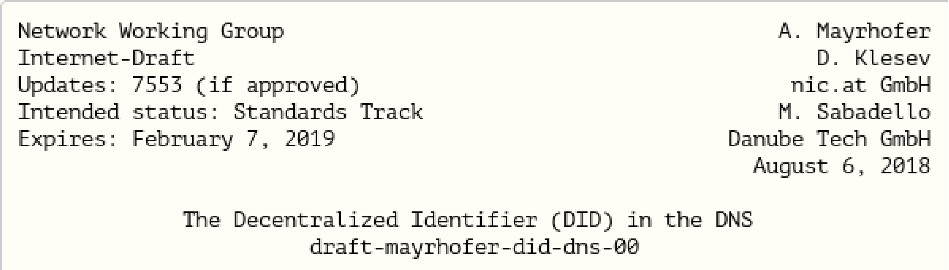
Other Topics:

- Versioning:
  - Input parameter to request specific version of DID Document, e.g. by version number, or by timestamp.
  - DID Document can contain version number or timestamp of last update.
- Caching:
  - Input parameter to request specific caching behavior, e.g. force fresh DID resolution.
  - Controlled by DID resolver configuration, input parameters, and DID Document content (“time-to-live”).
- Revocation:
  - DID resolver can return an error, or a DID Document with a “revoked” flag.
- Validation:
  - DID resolver validates DID Documents before returning them.
- Redirects:
  - DID can be used as the value of `serviceEndpoint`.

```
{
   "id": "did:btcr:x705-jzv2-qqaz-7vuz;hub",
   "type": "HubService",
   "serviceEndpoint": "did:btcr:xz35-jzv2-qqs2-9wjt"
}
```

Other Topics:

- Off-ledger DIDs (“microledgers”, “relationship state machine”):
  - DID method `did:sov:peer:` has been proposed
  - DID operations not in a public network, but between peers
- Which DID methods should a DID Resolver support?
  - DID Method Registry
- DID Names have been proposed.
- Petnames can point to DIDs.
- Domain names can point to DIDs:
  - DNS Resolution, e.g.: `_did.ssi.labs.nic.at.  300  IN  URI  10 1 "did:sov:stn:r1dwAJxcoG7EPiioGMz7h"`
  - WebFinger
  - HTML code in web page

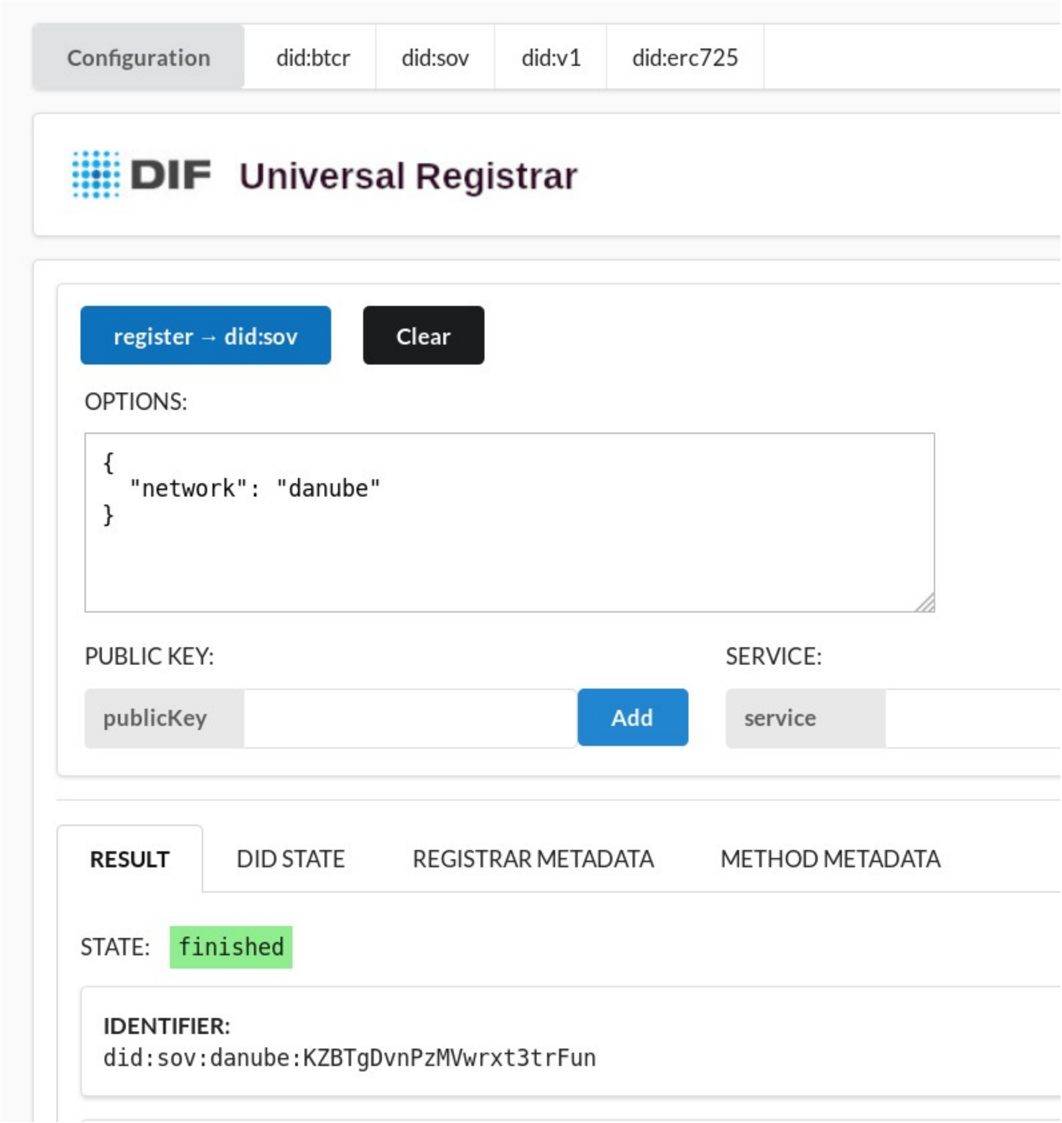


```
Network Working Group                                        A. Mayrhofer
Internet-Draft                                                  D. Klesev
Updates: 7553 (if approved)                                  nic.at GmbH
Intended status: Standards Track                             M. Sabadello
Expires: February 7, 2019                                Danube Tech GmbH
                                                           August 6, 2018

            The Decentralized Identifier (DID) in the DNS
                      draft-mayrhofer-did-dns-00
```

DID Universal Registrar

- Create/update/revoke a DID and 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.
- **https://uniregistrar.io/**



OPTIONS:

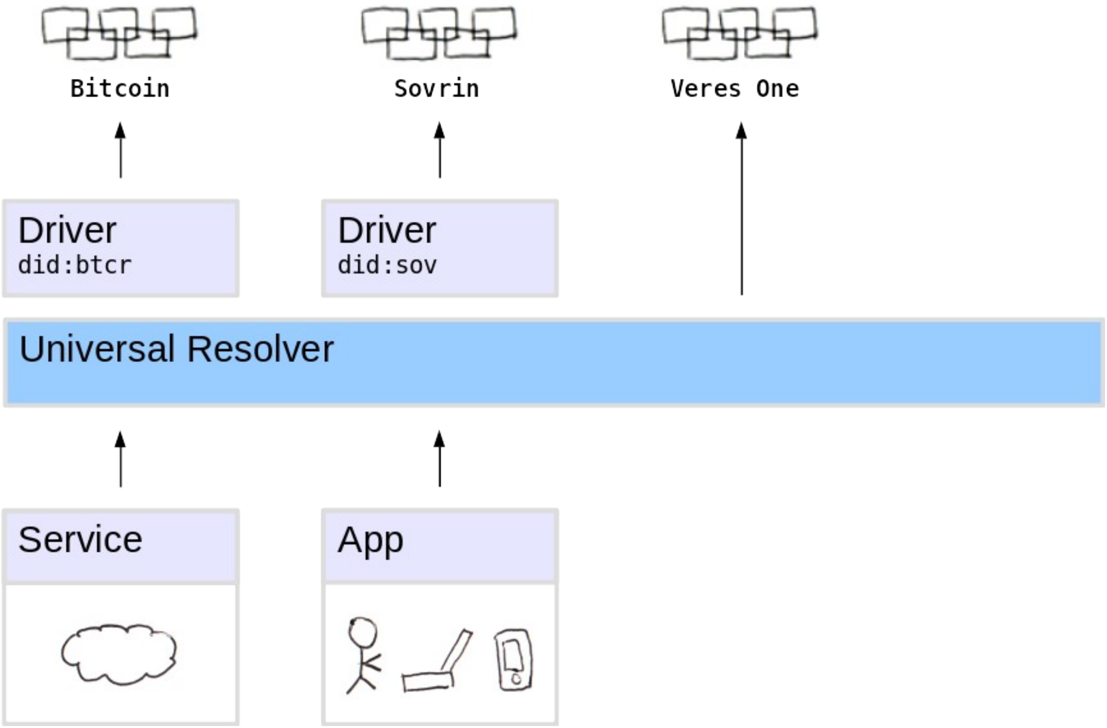
```
{
  "network": "danube"
}
```

STATE: finished

IDENTIFIER:
did:sov:danube:KZBTgDvnPzMVwrxt3trFun

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.
- **https://uniresolver.io/**



Sovrin

- Blockchain / DLT for Self-Sovereign Identity
- No cryptocurrency, no smart contracts
- Permissioned, public “global utility for identity”
- Used for DIDs, schemas, revocation
- Code based on Hyperledger Indy
- Governed by Sovrin Foundation

HYPERLEDGER INDY

sovrin

identity for all

Sovrin

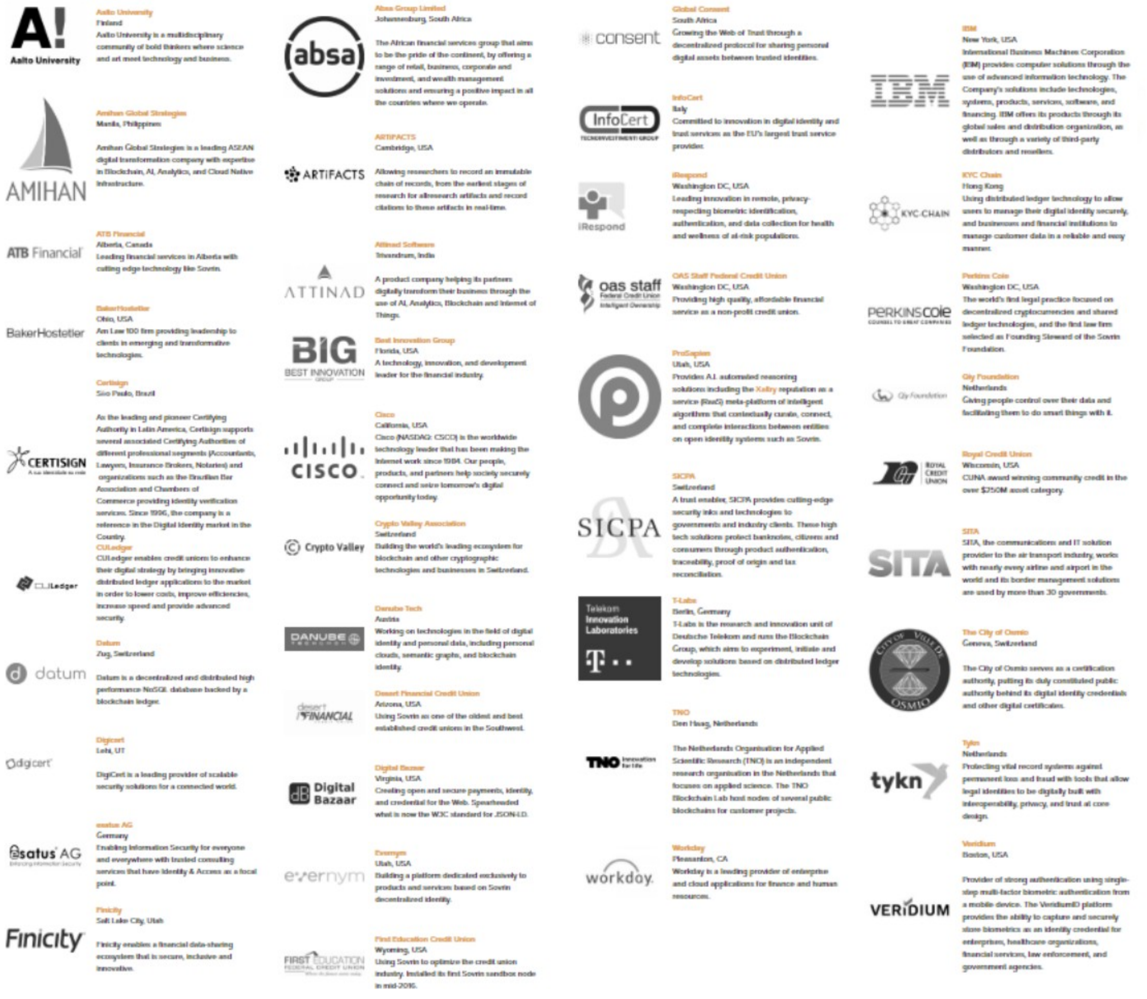
- About 40 "Stewards" who operate DLT nodes
- Financial institutions, certification authorities, tech companies, law firms, NGOs, universities, etc.

Who operates the ledger nodes?

Who can use the ledger?

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

* in permissionless mode



Aalto University
Finland
Aalto University is a multidisciplinary community of bold thinkers where science and art meet technology and business.

Amihan Global Strategies
Manila, Philippines

Amihan Global Strategies is a leading ASEAN digital transformation company with expertise in Blockchain, AI, Analytics, and Cloud Native Infrastructure.

ATB Financial
Alberta, Canada
Leading financial services in Alberta with cutting edge technology like Sovrin.

BakerHostetler
Ohio, USA
Am Law 100 firm providing leadership to clients in emerging and transformative technologies.

Certisign
São Paulo, Brazil

As the leading and pioneer Certifying Authority in Latin America, Certisign supports several associated Certifying Authorities of different professional segments (Accountants, Lawyers, Insurance Brokers, Notaries) and organizations such as the Brazilian Bar Association and Chambers of Commerce providing identity verification services. Since 1996, the company is a reference in the Digital Identity market in the Country.

CULedger
CULedger enables credit unions to enhance their digital strategy by bringing innovative distributed ledger applications to the market in order to lower costs, improve efficiencies, increase speed and provide advanced security.

Datum
Zug, Switzerland

Datum is a decentralized and distributed high performance NoSQL database backed by a blockchain ledger.

Digicert
Lehi, UT

DigiCert is a leading provider of scalable security solutions for a connected world.

esatus AG
Germany
Enabling Information Security for everyone and everywhere with trusted consulting services that have Identity & Access as a focal point.

Finicity
Salt Lake City, Utah

Finicity enables a financial data-sharing ecosystem that is secure, inclusive and innovative.

Absa Group Limited
Johannesburg, South Africa

The African financial services group that aims to be the pride of the continent, by offering a range of retail, business, corporate and investment, and wealth management solutions and ensuring a positive impact in all the countries where we operate.

ARTIFACTS
Cambridge, USA

Allowing researchers to record an immutable chain of records, from the earliest stages of research for allresearch artifacts and record citations to these artifacts in real-time.

Attinad Software
Trivandrum, India

A product company helping its partners digitally transform their business through the use of AI, Analytics, Blockchain and Internet of Things.

Best Innovation Group
Florida, USA
A technology, innovation, and development leader for the financial industry.

Cisco
California, USA
Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today.

Crypto Valley Association
Switzerland
Building the world's leading ecosystem for blockchain and other cryptographic technologies and businesses in Switzerland.

Danube Tech
Austria
Working on technologies in the field of digital identity and personal data, including personal clouds, semantic graphs, and blockchain identity.

Desert Financial Credit Union
Arizona, USA
Using Sovrin as one of the oldest and best established credit unions in the Southwest.

Digital Bazaar
Virginia, USA
Creating open and secure payments, identity, and credential for the Web. Spearheaded what is now the W3C standard for JSON-LD.

Evernym
Utah, USA
Building a platform dedicated exclusively to products and services based on Sovrin decentralized identity.

First Education Credit Union
Wyoming, USA
Using Sovrin to optimize the credit union industry. Installed its first Sovrin sandbox node in mid-2016.

Global Consent
South Africa
Growing the Web of Trust through a decentralized protocol for sharing personal digital assets between trusted identities.

InfoCert
Italy
Committed to innovation in digital identity and trust services as the EU's largest trust service provider.

iRespond
Washington DC, USA
Leading innovation in remote, privacy-respecting biometric identification, authentication, and data collection for health and wellness of at-risk populations.

OAS Staff Federal Credit Union
Washington DC, USA
Providing high quality, affordable financial service as a non-profit credit union.

ProSapien
Utah, USA
Provides A.I. automated reasoning solutions including the Xally reputation as a service (RaaS) meta-platform of intelligent algorithms that contextually curate, connect, and complete interactions between entities on open identity systems such as Sovrin.

SICPA
Switzerland
A trust enabler, SICPA provides cutting-edge security inks and technologies to governments and industry clients. These high tech solutions protect banknotes, citizens and consumers through product authentication, traceability, proof of origin and tax reconciliation.

T-Labs
Berlin, Germany
T-Labs is the research and innovation unit of Deutsche Telekom and runs the Blockchain Group, which aims to experiment, initiate and develop solutions based on distributed ledger technologies.

TNO
Den Haag, Netherlands

The Netherlands Organisation for Applied Scientific Research (TNO) is an independent research organisation in the Netherlands that focuses on applied science. The TNO Blockchain Lab host nodes of several public blockchains for customer projects.

Workday
Pleasanton, CA
Workday is a leading provider of enterprise and cloud applications for finance and human resources.

IBM
New York, USA
International Business Machines Corporation (IBM) provides computer solutions through the use of advanced information technology. The Company's solutions include technologies, systems, products, services, software, and financing. IBM offers its products through its global sales and distribution organization, as well as through a variety of third-party distributors and resellers.

KYC Chain
Hong Kong
Using distributed ledger technology to allow users to manage their digital identity securely, and businesses and financial institutions to manage customer data in a reliable and easy manner.

Perkins Coie
Washington DC, USA
The world's first legal practice focused on decentralized cryptocurrencies and shared ledger technologies, and the first law firm selected as Founding Steward of the Sovrin Foundation.

Qiy Foundation
Netherlands
Giving people control over their data and facilitating them to do smart things with it.

Royal Credit Union
Wisconsin, USA
CUNA award winning community credit in the over $750M asset category.

SITA
SITA, the communications and IT solution provider to the air transport industry, works with nearly every airline and airport in the world and its border management solutions are used by more than 30 governments.

The City of Osmio
Geneva, Switzerland

The City of Osmio serves as a certification authority, putting its duly constituted public authority behind its digital identity credentials and other digital certificates.

Tykn
Netherlands
Protecting vital record systems against permanent loss and fraud with tools that allow legal identities to be digitally built with interoperability, privacy, and trust at core design.

Veridium
Boston, USA

Provider of strong authentication using single-step multi-factor biometric authentication from a mobile device. The VeridiumID platform provides the ability to capture and securely store biometrics as an identity credential for enterprises, healthcare organizations, financial services, law enforcement, and government agencies.