

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





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

"Missing Identity Layer"



“Control, Consent, Context, Persistence, Portability, Pluralism”

Decentralized Identifiers (DIDs)

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:sov:3k9dg356wdcj5gf2k9bw8kfg7a



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"
    ]
  }
}
```

DID Methods

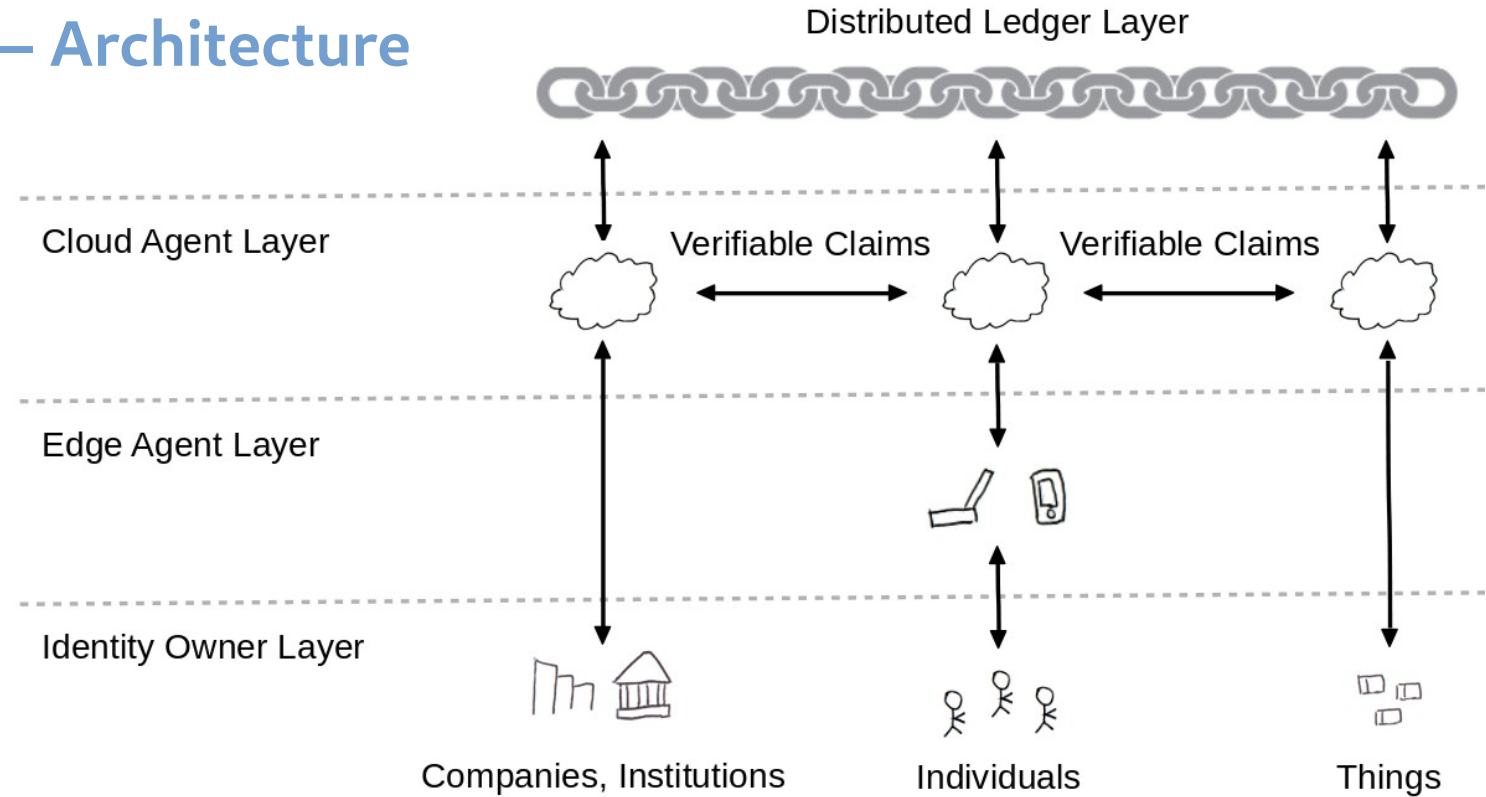
- Different DID “methods”:
- **did:sov, did:btcr, did:v1, did:uport, ...**
- All methods need:
 - A DID method specification (W3C)
 - An implementation of a “resolver”
- Define method-specific syntax
- Define CRUD for DIDs:
 - Create, Read (Resolve), Update, Delete (Revoke)

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:

Hyperledger Indy and Sovrin



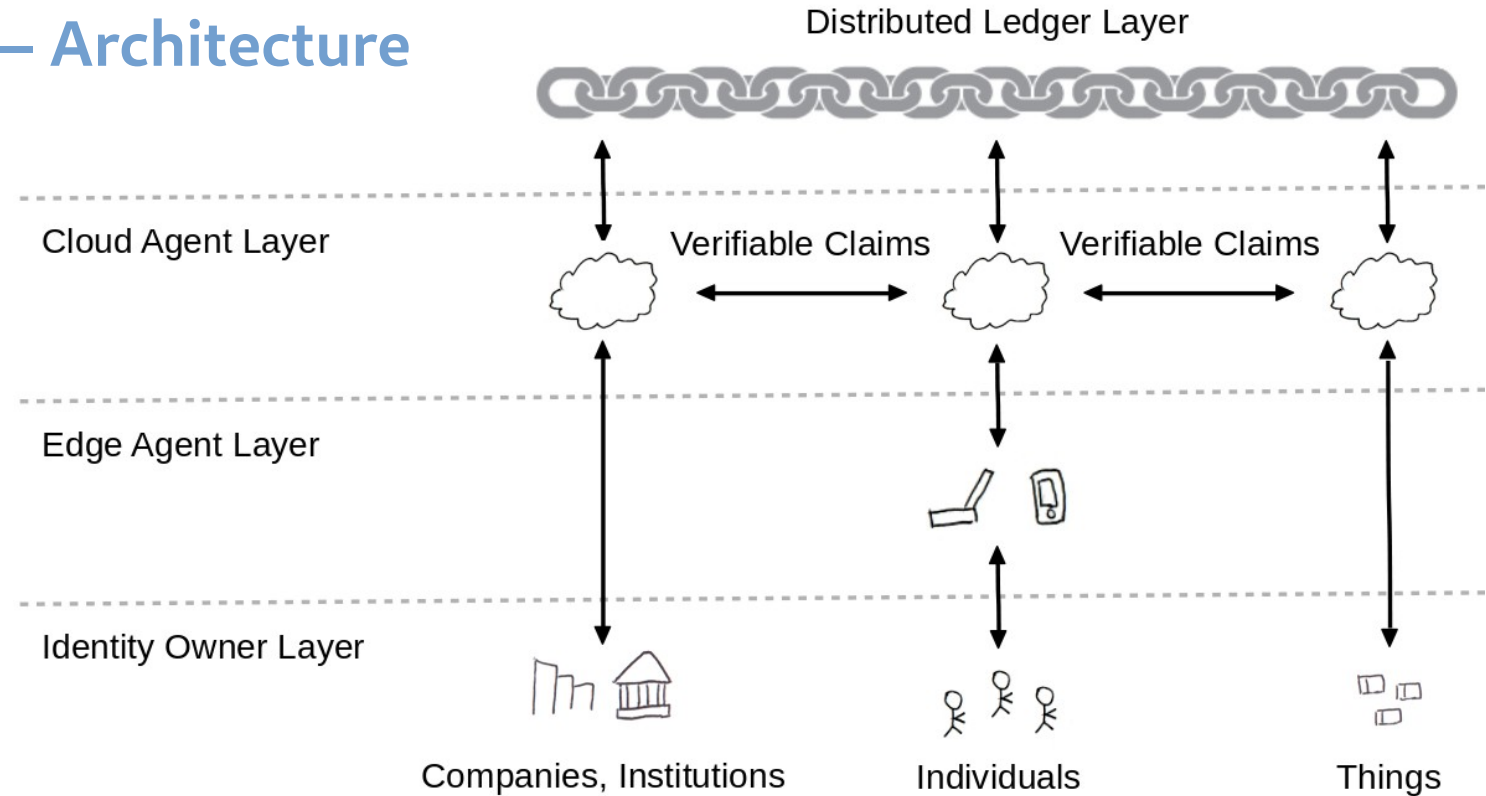
Hyperledger Indy – Architecture



HYPERLEDGER
INDY

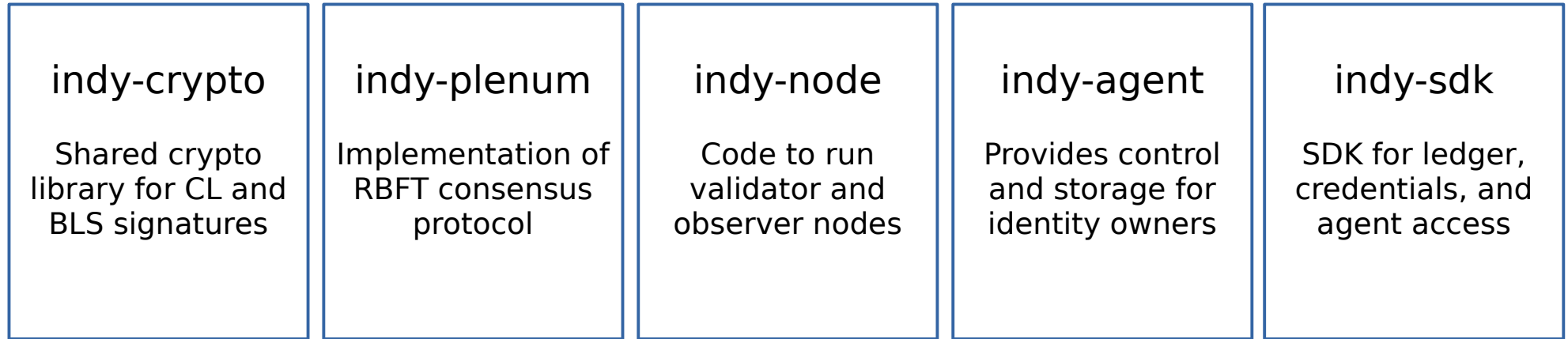
Hyperledger Indy – Architecture

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



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."



Includes wrappers and CLI



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 | ~4aSkMKFZHmFfwepDuco2b | -        |
+-----+-----+-----+
| 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

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

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

Who can use the ledger?

Who operates the ledger nodes?

	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 Strategist
Manila, Philippines
AMIHAN Global Strategist 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
An Law 100 firm providing leadership to clients in emerging and transformative technologies.



CERTISIGN
Los Angeles, CA
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.



CU Ledger
Chicago, IL
CU Ledger 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
Little, 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
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 irrefutable chain of records, from the earliest stages of research to the subsequent efforts and record claims to these artifacts in real-time.



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



BIG
BEST INNOVATION
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 1986. Our people, products, and partners help society securely connect and enjoy 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
Austria
Working on technologies in the field of digital identity and personal data, including personal clouds, semantic graphs, and blockchain identity.



dcmf FINANCIAL
Austria, USA
Using Sovrin as one of the oldest and best established credit unions in the Southwest.



db Digital Bazaar
Virginia, USA
Creating open and secure payment, identity, and credential for the Web. Sponsored 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
Wyoming, USA
Using Sovrin to optimize the credit union industry. Installed the first Sovrin sandbox node in mid 2016.



consent
Global Consent
New York, USA
Consent is 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.



lifespond
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
Providing high quality, affordable financial services as a non-profit credit union.



Prologika
Utah, USA
Provides AI, automated reasoning solutions including the *Kelly* reputation as a service (*Prolog*) meta platforms of intelligent algorithms that continuously create, connect, and complete interactions between entities on open identity systems such as Sovrin.



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



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



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



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



IBM
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
Washington DC, USA
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 COLE
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."



Q4 Foundation
Netherlands
Giving people control over their data and facilitating them to do smart things with it.



ROYAL UNION
Whitman, USA
Providing a secure 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 Chêne
Geneva, Switzerland
The City of Chêne serves as a certification authority, putting its fully constitutional public authority behind its digital identity credentials and other digital certificates.



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



Veridian
Boston, USA
Provider of strong authentication using single-step multi-factor biometric authentication from a mobile device. The VeridianE 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.

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>



Thank You

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



Extra Slides

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

- Edward Snowden



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."



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

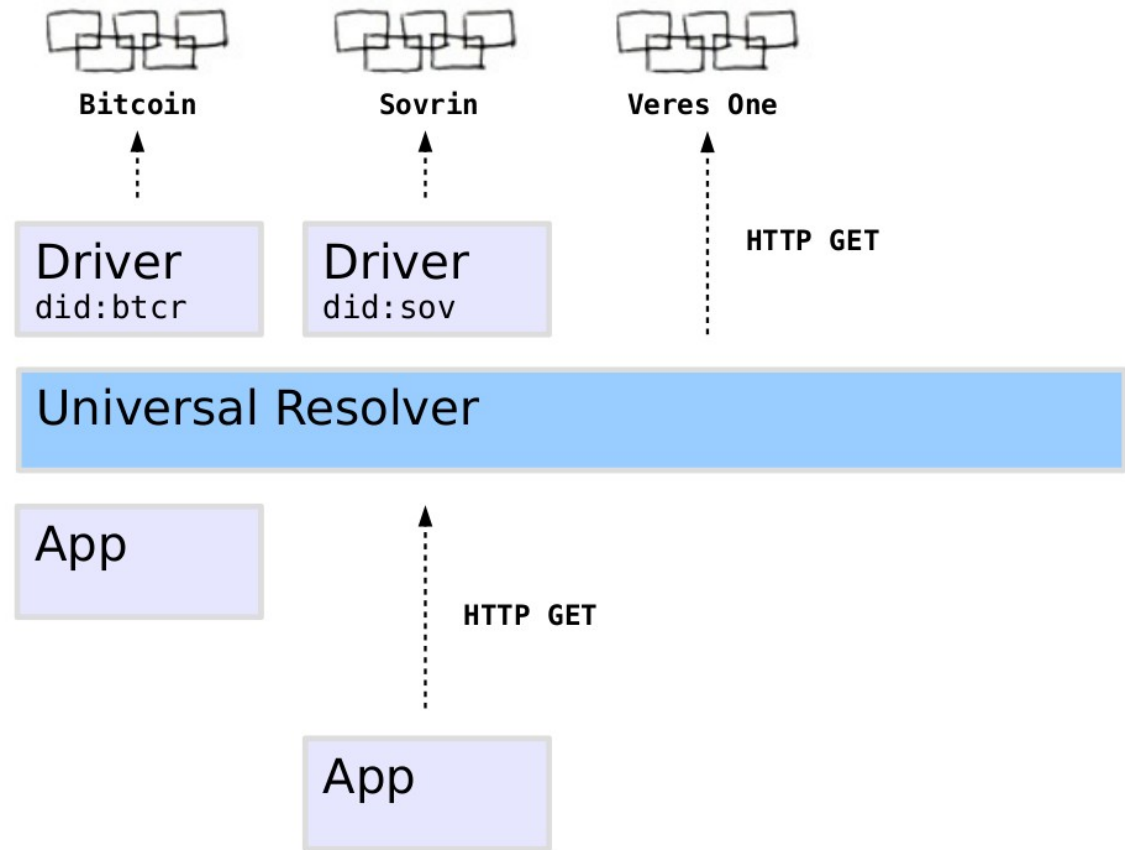


Craig Newmark
Founder, Craigslist

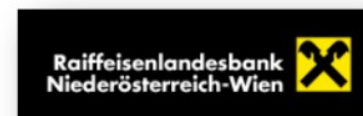
*"I'd like to use
[**blockchain**] for
verifiable identity."*

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/>



Proof-of-Concept: myIDsafe



Proof-of-Concept: myIDsafe



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.

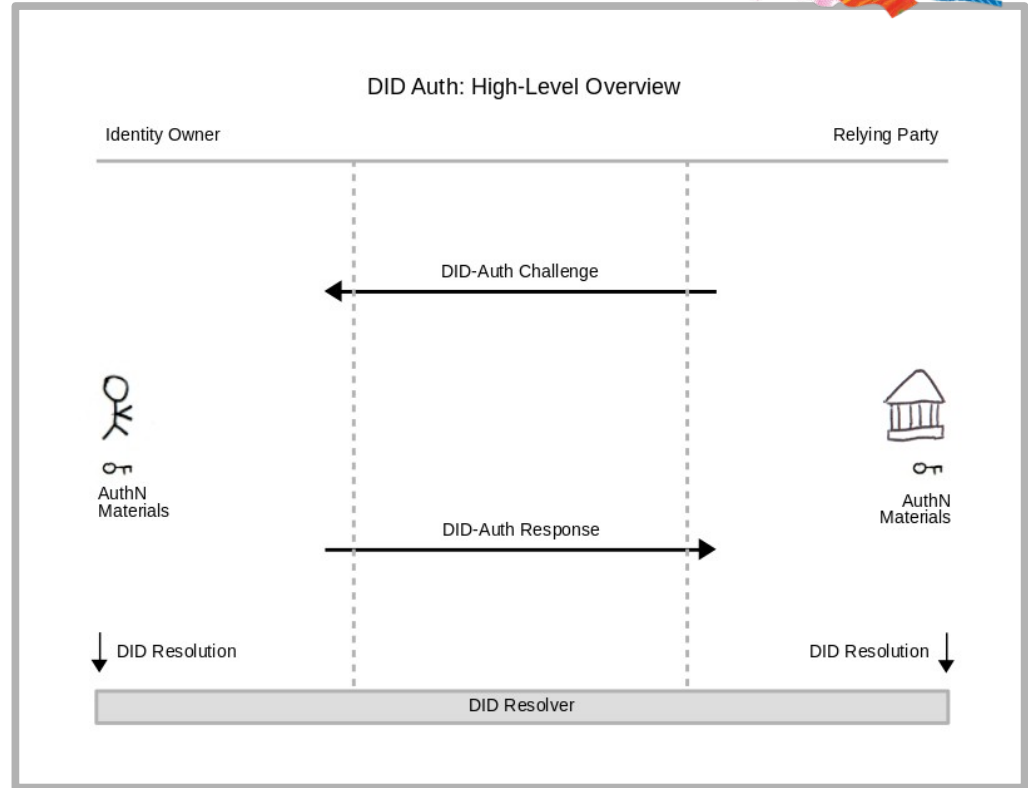
DID Auth

- 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

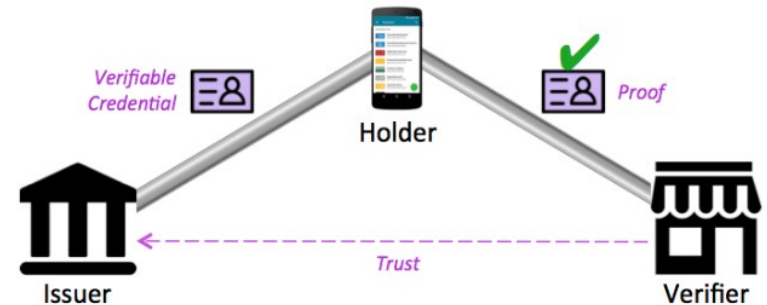
A White Paper from Rebooting the Web of Trust VI

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



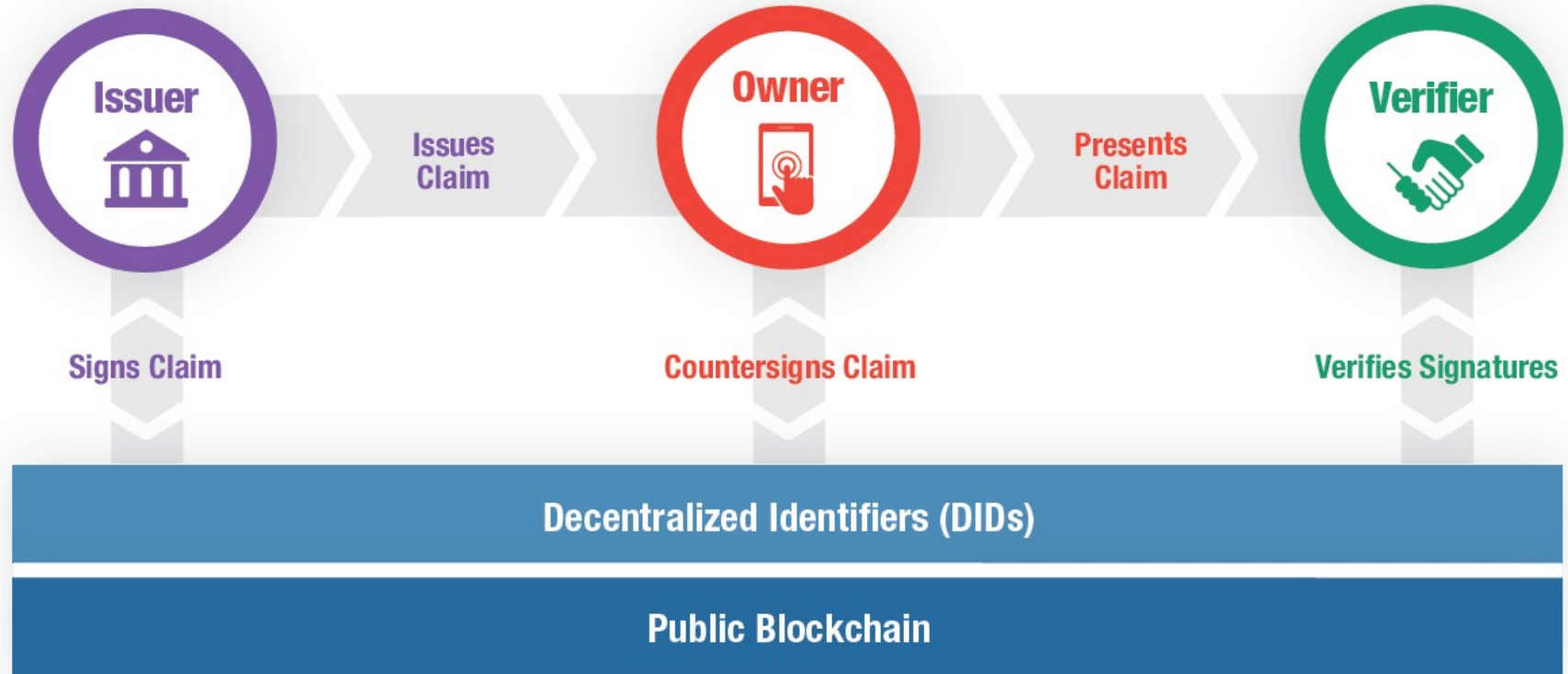
Verifiable Credentials

- 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”

Verifiable Credentials



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:btc:x6lj-wzvr-qqr-v-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/sCne04Jugez8RwDg/+
      MCRVpj0boDoe4SxxKjkC0vKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
      PRdW+gGsutPTLzvueMwmFhwYmfIFpbBu95t501+rSLHIEuuJM/+PXr9Cky6Ed
      +W3JT24="
  }
}
```

Verifiable Credentials



DKMS, DID Auth

Hubs, Agents, XDI



DIF



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



W3C JSON-LD 1.1

W3C Cryptographic Suites

RFC 7517: JWK



DID registered
prov. URI scheme



DID method specs

